LAUREA AMMATTIKORKEAKOULU Uuden edellä

WLAN-verkon suojaus VPN-yhteyden avulla

Ahtiainen, Jukka &
Ekblad, Kim

2014 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

WLAN-verkon suojaus VPN-yhteyden avulla

Ahtiainen Jukka &
Ekblad Kim
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Toukokuu, 2014

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Ahtiainen, Jukka &
Ekblad, Kim

WLAN-verkon suojaus VPN-yhteyden avulla

Vuosi 2014 Sivumäärä 51

Opinnäytetyössä käsitellään langattomia lähiverkkoja ja näiden salaustekniikoiden suojaustasoa. Ratkaisuksi tietoturvan varmistamiseksi esitetään VPN-yhteyden käyttämistä verkkoliikenteen sisällön suojaamiseksi, varsinkin käytettäessä avoimia WLAN-verkkoja. Työssä tutustutaan ensin langattomien lähiverkkojen (WLAN) eri versioihin ja salausratkaisuihin. Tämän jälkeen syvennytään VPN-tekniikkoihin, salausprotokolliin ja sertifikaatteihin.

Toiminnallisen opinnäytetyöosuuden asiakkaana toimi NextMesh International Oy. Yritys haluaa selvittää mahdollisuutta VPN-yhteyksien tarjoamiseen yrityksen ylläpitämissä WLAN-verkoissa. NextMesh International on tekniseltä osalta valmis tuomaan asiakkaidensa saataville VPN-asiakasyhteydet, jolloin julkisen verkon data saadaan suojattua. Palvelu tunnetaan myös Hotspot-suojauksena.

Opinnäytetyön aikana tutkittiin VPN-asiakasyhteyden toteutettavuutta, toimivuutta ja turvallisuutta käyttäen NextMesh Internationalin laitteistoa. Osana opinnäytetyötä syvennyttiin ohjelmoinnin kautta luotavaan yritysasiakkaalle räätälöityyn VPN-asiakasohjelmaan. Kolmannen osapuolen VPN-asiakasyhteysohjelmia testattiin usealla käyttöjärjestelmällä.

Asiasanat: Hotspot, Mobiilitietoturva, Tietoturvallisuus, Verkkoprotokollat, VPN, WLAN

Laurea University of Applied Sciences **Abstract**
Leppävaara
Bachelor's Degree Programme in Business Information Technology

Ahtiainen, Jukka &
Ekblad, Kim

Securing WLAN networks by VPN connection

Year 2014 Pages 51

This thesis focuses on wireless local area networks and the related encryption techniques. Virtual Private Network (VPN) connections are proposed as a solution to ensuring the security of information over networks, especially when using open WLAN-hotspots. The thesis first examines various versions of wireless local area networks (WLAN) and their encryption solutions. After these VPN techniques, encryption protocols and certificates are studied.

NextMesh International Oy was the client for the functional section of this thesis. The client company would like to examine the possibility of providing VPN connections over the networks they administer. NextMesh International is already able to bring VPN client connections to their clients, enabling information security over public networks. The service is known as Hotspot shielding.

The implementability, functionality and security of VPN client connections were studied during the thesis project using hardware provided by NextMesh International. The customization of VPN client software for the client company by programming was also part of the project. Third party VPN client applications were tested on different operating systems.

Keywords: Hotspot, Information security, Mobile networking, Network protocols, VPN, WLAN

Sisällys

1 Johdanto 6
1.1 Taustatiedot 7
1.2 OSI-malli 7
1.3 Yksityisyydensuoja 8
2 WLAN 9
2.1 802.11g 11
2.2 802.11n 11
2.3 802.11ac 12
2.4 WEP, WPA & WPA2 12
3 VPN 14
3.1 VPN-protokollat 15
3.2 VPN-asiakasohjelma 15
3.3 VPN-palvelin 16
3.4 Sertifikaatit 17
3.5 Tietoturvallisuus 18
4 WLAN:in suojaus VPN-tunneloinnilla 19
4.1 NextMesh International verkkoasiakas 23
4.2 WLAN-tukiasema 23
4.3 Reititin 24
5 Verkkosuojausten testaus 25
5.1 Langattoman verkon suojauksen murtaminen 26
5.2 WLAN-verkkoon murtautuminen käytännössä 27
5.3 Verkkoliikenteen tulkinta 29
5.4 VPN-ohjelmistojen turvallisuus 31
6 VPN-ohjelmistototeutus 33
6.1 VPN-ohjelmistototeutuksen rajaukset 34
6.2 VPN-käyttöliittymän kehykset 35
6.3 Ohjelmiston rakenne 36
6.4 Toteutuksen ohjelmisto 37
6.5 Ohjelmistonkehitysympäristö 38
6.6 Vaihtoehtoiset toteutukset 38
7 Yhteenveto 39
Lähteet 43
Kuvaluettelo 46
Taulukot 46
Liitteet 46

1 Johdanto

Langattomien verkkojen suojaukset ovat jääneet kehityksessä ajastaan jälkeen. WPA2 (WiFi Protected Access II) on jo kymmenvuotias ja edelleen käytössä oleva suojausprotokolla. Nykyisillä tietokoneilla ja verkkotyökaluilla nämä suojaukset ovat kuitenkin liian helposti murrettavissa, kuten kappaleessa 5.2 todistetaan. Lisäksi useat tahot tarjoavat avoimia suojaamattomia WLAN-verkkoja asiakkailleen. Opinnäytetyö käsittelee langattoman WLAN-verkon suojausta VPN-palvelun (Virtual Private Network) avulla.

Verkkovierailuja tehdään jopa työlaitteilla, esimerkiksi työmatkalla on helppo yhdistää kannettava tietokone tai älypuhelin avoimeen WLAN-verkkoon sähköpostin lukemista varten. Vaihtoehtoisesti olisi ulkomailla käydessä hankittava paikallinen mobiililiittymä. Avoin suojaamaton WLAN-verkko on tietoturvan kannalta suuri riski. Tämänkaltaista verkkoa käytettäessä voidaan pahimmillaan paljastaa yrityssalaisuuksia ja henkilökohtaisia tietoja.

Tietoturvaa voidaan parantaa huomattavasti ottamalla käyttöön VPN-palvelu joka salaa automaattisesti käyttäjän liikenteen. Useat kaupalliset toimijat ympäri maailman tarjoavat eri hinnoitteluperiaatteilla palveluita, joihin usein kuuluu asiakasohjelma. Myös ilmaisia palveluja löytyy, mutta nämä kärsivät hitaudesta ja palvelun luotettavuudesta ei aina ole takeita.

NextMesh tarjoaa palveluna asiakkailleen WLAN-verkkoja, esimerkiksi kauppakeskuksissa. Nämä WLAN-verkot ovat suojaamattomia, mutta valmius VPN-yhteyksiin on jo olemassa. Eri suojausprotokollia tutkittiin paljon ja VPN-yhteyksien käytännön toimivuutta testattiin NextMeshin laitteistolla. Projektin vetäjänä NextMeshillä toimi tuotantopäällikkö Mika Järvinen.

Käytännön kokeissa havaittiin WLAN-verkkoja suojaavan WPA2-suojauksen riittämättömyys ainoaksi suojauskerrokseksi. Myös HTTPS-protokollalla suojattu liikenne osoittautui alttiiksi salakuuntelulle. VPN-yhteyden kyky suojata verkkoliikenne erivahvuisilla salausalgoritmeilla tarjoaa luotettavimman suojan. Lisäksi VPN-palvelin piilottaa asiakkaan IP-osoitteen, lisäten turvallisuutta internetissä.

Työn teoriaosuudessa käsitellään OSI-mallia ja WLAN sekä VPN tekniikoita. Työ yhdistää WLAN ja VPN tekniikat toteutuksellisessa osuudessa. Työssä keskitytään langattomien verkkojen tekniseen tietoturvaan. Tekniikoita voi kuitenkin soveltaa kaikissa eri verkoissa. Teoriaosuuden jälkeen testattiin työssä käsiteltyjä tekniikoita käytännössä. Työn aikana syvennyttiin WLAN VPN sovelluksen ohjelmointiin Androidille. Ohjelmistoa pystyttiin menestyksekkäästi testaamaan, mutta testausten tuloksena ei valmistunut julkaisukelpoista Alpha-versiota. Työn

aikana pyrittiin myös testaamaan todennäköisimpiä verkkohyökkäyksiä. Työssä käytetyt lyhenteet ovat selitettynä liitteessä 1.

1.1 Taustatiedot

Opinnäytetyö sisältää huomattavan määrän vieraita termejä, standardeja ja protokollia. Termit avataan käytetyissä lyhenteissä ja osittain itse tekstissä. OSI-malliin viitataan työssä usein selkeyttämisen vuoksi. WLAN ja VPN käsitellään myös yksityiskohtaisesti, jotta ymmärretään VPN-WLAN-tietoturvasovelluksen lähtökohdat. Teoreettisesti paneudutaan myös varmenteisiin, eli sertifikaatteihin. Käsittelyssä ovat olennaisesti myös tietoturvallisuus sovelluksen osalta ja toteutukseen liittyvät rajaukset. Työstä rajattiin Androidia lukuun ottamatta muut käyttöliittymät pois. Opinnäytetyössä käytetyt lyhenteet ovat liitteessä työn lopussa. (Ks. Liite 1.)

WLAN, WiFi, hotspot ja 802.11 tarkoittavat käytännössä kaikki samaa asiaa, langatonta verkkoa. Langattomat verkot ovat yleistyneet räjähdysmäisesti Steven Jobsin iBook ajoista vuodesta 2000. Jobs esitteli hauskasti hulavanteen avulla iBook-laitteen langattomuuden ja sensaatiomaisen tavan liittyä verkkoon. Langattomien verkkojen kommunikoinnin polkaisi käyntiin Norman Abramson. Hän kehitti Havaijin yliopistolla työryhmänsä kanssa ALOHANET-verkon Havaijin saariryhmälle jo 1971. (University of Hawaii 2013.)

Varmaa lukumäärää maailmanlaajuisesti käyttäjistä, jotka vierailevat WLAN-verkossa ei ole saatavilla. NextMesh Internationalin yhdessä useista hotspot verkoista kauppakeskus Isossa omenassa vierailee päivittäin muutama sata käyttäjää. Kuukaudessa kävijöitä on vajaat kymmenen tuhatta (NextMesh International Oy). Yritysmaailman WLAN-verkkojen vuosittaisesta jatkuvasta kasvusta kertovat tilastot. WLAN markkinoiden kasvu on hieman hidastunut yli 20 % kasvun keskiarvosta, mutta esimerkiksi Ciscon tulos 16,7 % näyttää selkeää kasvua. (Shirer 2013.)

1.2 OSI-malli

OSI-malli kehitettiin tietoliikennejärjestelmän pohjaksi. Siinä on kehykset tietoliikenneyhteyksille. OSI-malli ei ole kaupallinen tuote. OSI-mallin kehitti ISO (International Standardization Organization). OSI-malli, eli (Open Systems Interconnection) sisältää seitsemän kerrosta. Nämä kerrokset on nimetty alhaalta ylös seuraavasti: fyysinenkerros, siirtoyhteyskerros, verkkokerros, kuljetuskerros, yhteysjaksokerros, esitystapakerros ja sovelluskerros. (Ala-Mutka, Rintala, Savikko & Palviainen 2002.) Kerroksilla on omat rajapintansa, jotka välittävät viestejä ylä- ja alapuolella oleville kerroksille pyyntöinä, tiedusteluina tai vahvistuksina. (Ratol 2002.)

Kuva 1: OSI-malli

OSI-mallin avulla havainnollistetaan VPN:n yhteyskäytäntöjä. Näin ymmärretään paremmin, kuinka VPN toimii. NextMesh Internationalin reitittimet ja hotspot-alueiden WLAN-tukiasemat toimivat OSI-mallin fyysisessä kerroksessa.

OSI-mallin toisessa kerroksessa luodaan VPN-tunneli. Verkkokerros vastaa käyttäjän datan kulusta salattuna. Korkeammissa kerroksissa data ilmenee taas salaamattomana ja sovellukset pystyvät esittämään käyttäjälle selkokielistä tekstiä. (Spamlaws 2013.)

1.3 Yksityisyydensuoja

Verkkovierailut joita tehdään työmatkojen tai lomamatkojen aikana ovat kasvava tietoturvallisuusriski. Työsähköposteista tai yksityisistä sähköpostitileistä luettu data on aina vaarassa julkisen verkon yli luettaessa. Tietoturvallisuuteen vihkiytymätön käyttäjä saattaa huoletta lukea kaikki postinsa läpi paikallisen kahvilan WiFi-verkossa. VPN-asiakasohjelman muodostamalla verkkoyhteydellä luetut sähköpostit julkisessa WiFi-verkossa ovat puolestaan riittävällä tasolla suojatut.

Yksityisyydensuoja on useilla käyttäjillä olematonta esimerkiksi Googlen, Facebookin tai Skypen palveluiden osalta. USA:ssa tuotettujen ohjelmistojen tietoturva on käytännössä murrettu NSA:n toimesta (National Security Agency). Lisäksi Internetissä on paljon vakoiluohjelmia, joiden kautta NSA louhii järjestelmällisesti tietoa. Käytössä olevia ohjelmistoja on useita

kymmeniä. Näitä ovat muun muassa XKeyScore, PRISM, Cybertrans, Doublearrow ja Yellowstone.

Marcus Ranumin mukaan ”Yhdysvallat kohtelee Internetiä, kuin yhtä siirtomaistaan. Olemme ikään kuin palanneet siirtomaa-aikaan ja meidän tulisi ajatella amerikkalaisia isäntinämme.” (Hyppönen 2013.) Yhdysvallat eivät suinkaan ole tiedustelupalveluita ainoa huomattavasti hyväksikäyttävä valtio. Meitä suomalaisia läheisesti koskettava Ruotsi on myös taannut omalla laillaan, että Ruotsin tiedustelupalvelu voi analysoida kaiken Ruotsin kautta kulkevan dataliikenteen. Suomesta valtaosa tietoliikenteestä kulkee Ruotsin kautta. Näin ollen Ruotsin tiedustelupalvelu voi toistaiseksi kerätä kaiken datan, mitä Suomesta kulkee ulkomaille, laillisesti. Ruotsin lait ovat hyvin samankaltaiset kuin Yhdysvaltojen. Yhdysvalloissa laki sallii datan keräämisen ja analysoinnin ulkomaalaisilta, mikäli data kulkee Yhdysvaltojen kautta tai päätyy Yhdysvaltoihin. Käytännössä tämä tarkoittaa sitä, että USA:n tiedustelu kerää dataa 96 %:sta maailman väestön tietoja. Esimerkiksi Skype oli ennen myyntiään Yhdysvaltoihin yksityisyyttä suojaava sovellus. Nykyisten tietojen valossa tämäkin sovellus on käytännössä täysin USA:n tiedustelupalvelun hallittavissa. (Hyppönen 2013.)

Nykyisten paljastusten valossa tiedetään myös USA:n tiedustelun soluttautumisista standardointijärjestöihin. He ovat järjestelmällisesti sabotoineet datan salausmenetelmiä asentaen ohjelmistoihin ja sovelluksiin takaportteja, joista he pääsevät kulkemaan kenenkään asiaa tietämättä. Tästä johtuu muun muassa tietoturvayhtiö RSA:n kehotus asiakkailleen olla käyttämättä heidän salaustuotteitaan, joissa ilmeni NSA:n tekemiä takaportteja. (Goodin 2013.)

2 WLAN

WLAN:ia ymmärtääkseen tulee ensin ymmärtää LAN-määritelmä. Local Area Network, eli lähiverkko muodostetaan älylaitteiden tai koneiden ryhmistä. LAN-määritelmä käsitetään nykyisin maantieteellisesti hyvin pienelle ja rajatulle alueelle tehdystä lähiverkosta. Esimerkiksi toimitalo tai yksityisasunto ovat paikkoja, joissa LAN on edelleen käytännöllinen nopeutensa ja turvallisuutensa vuoksi. LAN-verkon vastakohta on WAN, eli Wide Area Network. WAN kuvaa käytännössä Internetiä sellaisena, kuin sen nykyisin ymmärrämme. Lähiverkoista WLAN ympäristöiksi on kehitys vienyt käyttäjien tarpeiden mukaan. LAN, WAN ja WLAN ovat myös käytetyt lyhenteet liitteessä opinnäytetyön lopussa. Työpaikoilla on siirretty työasemat WLAN ympäristöiksi käytännössä kustannustehokkuuden vuoksi ja kotitalouksissa puolestaan WLAN-verkon asennuksen helppous ja mobiililaitteiden liikuteltavuus on käytännössä syrjäyttänyt kaapeliverkot. (Al Shourbaji 2013.)

Langattomista lähiverkoista käytetään lyhenteitä WLAN ja WiFi. WLAN, joka on yleisesti käytössä Suomessa, tulee sanoista Wireless Local Area Network kun taas WiFi, joka on suositumpi

mm. Yhdysvalloissa ja osissa Aasiaa, tulee sanoista Wireless Fidelity joka puolestaan juontuu äänentoistoon liittyvästä sanasta HiFi (High Fidelity). WLAN-verkot perustuvat IEEE 802.11-standardeihin (Institute of Electrical and Electronics Engineers) ja liikennöivät lisenssivapailla radiotaajuuksilla tukiaseman ja asiakkaan välillä. (Koivunen 2010.)

WLAN-verkon liikenne ei itsessään ole suojattua vaan vaatii valinnaisen tekniikan tietoturvallisuuden takaamiseksi. 802.11-standardin mukaisia tekniikoita on tarjolla useampikin. Isommissa organisaatioissa voidaan käyttää keskitettyä käyttäjätunnistusta (802.11x) mutta pienemmät langattomat verkot suojataan yleensä jaettua avainta käyttäen. (Bartz 2012.)

Jaettuun avaimeen perustuvat 802.11-standardin mukaiset tekniikat ovat WEP (Wired Equivalent Protection), WPA (Wi-Fi Protected Access) ja WPA2. WEP on todettu haavoittuvaksi ja tekniikka on muutenkin vanhentunut. WPA2 on suojaustasoltaan parempi kuin WPA, mutta vanhempien laitteiden yhteensopivuuden takaamiseksi nykyisissä käyttöjärjestelmissä, on WPA edelleen paikoitellen käytössä. (Bartz 2012.)

802.11i-standardi on 802.11-verkkojen tuorein suojausstandardi josta WP2 juontuu. Jaettuun avaimeen edelleen perustuva tekniikka soveltaa WPA:sta poiketen AES-salausmenetelmää. WPA2:n todennusmenetelmä on lainattu 802.11x-standardista, josta on myös seurausta avaintenhallintakäytäntö. (Bartz 2012.)

Jaettuun avaimeen perustuvat suojaustekniikat eivät kuitenkaan sovellu kaikkiin tilanteisiin. Avoimet yleiseen käyttöön tarkoitetut WLAN-verkot ovat useimmiten täysin suojaamattomia. Vaihtoehtoisesti ne käyttävät jotakin kolmannen osapuolen tarjoamaa suojaustekniikkaa. (Lanning 2007.)

Opinnäytetyön asiakas NextMesh Internationalin käyttämät tukiasemat tukevat IEEE 802.11n ja 802.11g standardeja. Näistä tuoreempi 802.11n tarjoaa nopeamman yhteyden lisäksi paremman kuuluvuuden. NextMesh International tarjoaa kauppakeskuksille avoimia hotspot WLAN-verkkoja, mutta ilman salausta (NextMesh International 2013). Jaetun avaimen hankkiminen on potentiaaliselle WLAN-vierailijalle hidaste ja saattaa johtaa usein siihen, että verkkovierailu jätetään tekemättä. (Lanning 2007.)

WLAN:in tulevaisuus vaikuttaa vahvalta. WLAN on kehittynyt nykypäivän kommunikaation ratkaisuksi. Sisäiset yritysverkot ja avoimet julkiset verkot muuttuvat jatkuvasti langattomaan suuntaan. Standardien ja protokollien yleistyminen tukevat WLAN ympäristöä eteenpäin. Ikuisena haasteena on hakkereiden olemassa olo. Niille ei kukaan voi mitään, mutta jatkuva kehitys WLAN tietoturvatekniikoissa tekee myös hakkereiden työn vaikeaksi. Passiivisesti dataa keräävät hakkerit ovat normaalia vaarallisempia. He keräävät verkon varjoissa dataa ennen

hyökkäyksen käynnistystä. Tämänkaltaista hyökkäystä vastaan ei voi suojautua muutoin, kuin käyttämällä jatkuvasti mahdollisimman korkealuokkaista datan salausta. (Al Shourbaji 2013.)

2.1 802.11g

802.11g on vuonna 2003 standardoitu langaton lähiverkkotekniikka. 2,4GHz:n taajuusalueella toimiva OFDM-modulointia käyttävä tekniikka kykenee teoriassa 54Mbps tiedonsiirtonopeuteen. 802.11g standardia edelsi 802.11b standardi, jonka teoreettinen tiedonsiirtonopeus oli 11Mbps. (Bartz 2012.)

Dynamic Rate Scaling -toiminto määrää WLAN-verkon nopeuden. Mikäli kahden langattoman laitteen välinen yhteys ei ole vahva, ei yhteyskään ole teoreettisen maksimitiedonsiirtonopeuden mukainen. Tiedonsiirtonopeus laskee maksiminopeutta taulukon mukaan, joka on tehty jokaiselle standardille erikseen. (Mitchell 2013.)

Suhteellisen korkeasta iästään huolimatta on edelleen hyvä huomioida tämän tekniikan tuki langattomia lähiverkkoja perustettaessa, sillä tämän sukupolven tekniikalla varustettuja puhelimia on yhä käytössä. Pelkästään 802.11g tekniikalla varustettuja älypuhelimia ei enää kuitenkaan valmisteta. Nykyiset myynnissä olevat laitteet tukevat vähintään uudempaa 802.11n standardia. (Mitchell 2013.)

2.2 802.11n

802.11n on tällä hetkellä yleisin käytössä oleva langaton lähiverkkotekniikka. Ruuhkaisen 2,4GHz:n taajuusalueen lisäksi myös 5GHz:n taajuusalue on käytettävissä. Edeltävään standardisukupolveen verrattuna tiedonsiirtonopeutta on saatu kasvatettua varsinkin MIMO-tekniikalla (multiple-input multiple-output) ja laajentamalla käytettyjä radiokanavia. Laitteistosta riippuen enimmäissiirtonopeus on välillä 150Mbps ja 600Mbps. (Bartz 2012.)

802.11n-tekniikan nopeus riippuu käytettävien antennien määrästä MIMO-tekniikalla. Sekä lähettävässä että vastaanottavassa laitteessa on oltava neljä antennia teoreettisen maksimisiirtoyhteysnopeuden saavuttamiseksi. Antennien lukumäärää kasvattamalla pystytään myös vähentämään vastaanotossa tapahtuvia häiriöitä. Tulevaisuudessa tämä tulee ruuhkauttamaan myös 5GHz:n taajuusalueen, aivan kuten 2,4GHz:n taajuusalueen on jo käynyt taajama-alueilla. (Bartz 2012.)

Usealla vuodella myöhästynyt standardi aiheutti laitevalmistajissa hermostumista, joka johti epästandarditekniikoita käyttäviin laitejulkaisuihin. Vuonna 2009 IEEE sai standardin valmiik-

si. Siinä vaiheessa markkinoilla oli jo muutamia vuosia ollut tarjolla laitteita, jotka perustuivat löyhästi IEEE:n vedoksiin tulevasta standardista. (Bartz 2012.)

2.3 802.11ac

IEEE:n odotetaan saavan standardin viimeisteltyä vuoden 2013 viimeisellä neljänneksellä ja lopullinen hyväksyntä tapahtuu vuoden 2014 helmikuussa (McCann & Ashley 2013). Tämä seuraavan sukupolven langaton lähiverkkotekniikka kasvattaa tiedonsiirtonopeutta entisestään käyttäen leveämpää radiokaistaa, suurempaa rinnakkaissiirtoa (MIMO) ja kasvattamalla pakettien kehyskokoa.

Kuten edellisen sukupolven, 802.11n, tekniikan kanssa laitteita on tarjolla ennen varsinaista standardin valmistumista. Piirivalmistajat aloittivat tuotannon jo vuotta ennen odotettua standardinvalmistumisajankohtaa. 802.11ac-tekniikkaa tukevia laitteita löytyy tukiasemista älypuhelimiin asti. (Cisco 2012.)

802.11ac-tekniikka valmistettiin kasvavaa WLAN-verkon tarvetta varten. Mobiililaitteiden valtava myyntikasvu vaatii tehokkaampia langattomia verkkoja. Nykyisin kansainvälisissä yrityksissä henkilöä kohden on yli kaksi langattomassa verkossa toimivaa laitetta käytössä. (Meru Networks 2012.)

2.4 WEP, WPA & WPA2

WPA- ja WPA2-turvatekniikat ovat WLAN ja WiFi tietoturvastandardeja. Näitä suojausprotokollia tutkittiin, koska ne ovat yleisimpiä langattoman verkon suojaustekniikoita. WPA2-turvatekniikka ei kuitenkaan sovellu hotspot-verkon suojaamiseen. WPA2 on verkkovierailijalle liian hidas ja monimutkainen ottaa käyttöön. VPN on tietoturvallisuustekijöiltään paremmin hotspot-verkolle soveltuva tietoturvasovellusta tukevaksi, kuin WPA2-tietoturvatekniikka. (Bartz 2012.)

WEP on IEEE:n mukainen turvallisuusalgoritmi. 802.11i:n tuoma salausmenetelmä käyttää RC4-jonosalainta 64- tai 128-bittisellä avaimella. Verkon oma salasana tosin syö 40- tai vastaavasti 104-bittiä jättäen vain 24-bittiä alustusvektorille (IV, Initialization Vector). Langattoman verkon liikennettä seuraamalla saattoi selvittää salausavaimen jopa vuorokaudessa, sillä 24-bitillä samoja paketteja alkoi pian liikkua verkossa. (Järvinen, P. 2003.) MAC-osoitteiden, eli laitteiden fyysisten tunnisteiden, suodatus mahdollisti verkkoon pääsyn vain valituille laitteille. SSID:n, eli langattoman verkon tunnisteen, piilottaminen loi lähinnä näennäistä turvaa. WEP toimii OSI-mallin toisessa, eli siirtoyhteyskerroksessa. (Bartz 2012.)

WPA, eli Wi-Fi Protected Access kehitettiin alkuperäisten WLAN-standardien heikon tietoturvan paikkaamiseksi. WPA kehitettiin WEP turvallisuusalgoritmin suoraksi jatkeeksi. WPA toi mukanaan useita kehittyneitä tietoturvaominaisuuksia jotka muun muassa tarjosivat suuremmille organisaatioille langattomien verkkojen keskitetyn pääsynhallinnan. (Mitchell 2013.)

Vuonna 2003 WPA julkaistiin tietoisesti puolivalmiina. Wi-Fi Alliancen jäsenet halusivat mahdollisimman nopeasti saada markkinoille tietoturvaltaan ala-arvoisen WEP:in korvaajan. WPA toimii WEP turvallisuusalgoritmin tavoin OSI-mallin toisessa kerroksessa. (Bartz 2012.) WPA kumosi keskeneräisenäkin paremmalla salaustekniikallaan TKIP ja AES suojaukset, jotka olivat WEP-salausmenetelmän tukijalat. WPA:an kuului myös sisäänrakennettu todennustuki, jota WEP-salausmenetelmässä ei myöskään ollut. (Mitchell 2013.)

Vuonna 2004 WPA2 valmistui korvaamaan WPA-tekniikan ja lisättiin osaksi alkuperäistä 802.11i-standardia nimellä 802.11i-2004. Muutamaa vuotta myöhemmin IEEE ymppäsi WPA2:n tuomat tekniikat osaksi WLAN:ia yhdistävää standardia 802.11-2007. (IEEE 2007.)

Wi-Fi Alliancen turvatekniikka	**Autentikointitekniikka**	**Salaustekniikka**
WPA – Personal	Salasana	TKIP/RC4
WPA – Enterprise	802.1X/EAP	TKIP/RC4
WPA 2.0 – Personal	Salasana	CCMP/AES tai TKIP/RC4
WPA 2.0 – Enterprise	802.1X/EAP	CCMP/AES tai TKIP/RC4

Taulukko 1: WPA/WPA2-turvatekniikat (Bartz 2012.)

Yllä olevasta taulukosta selviää, että sekä WPA, että WPA2 tarjoavat erilliset tekniikat kodin tai pientoimiston ja yrityksen tai organisaation langattoman tietoturvan hallintaan. WPA2-turvatekniikka takaa edelleen riittävän turvallisen suojan niin koti- kuin yrityskäyttöönkin. WPA-turvatekniikka on murrettu useiden tieteellistenkin tahojen toimesta alle varttitunnissa. WPA2 on toistaiseksi niin työläs tekniikka murrettavaksi, että pahantahtoiset hakkerit hakeutuvat nopeammin murtuvien standardien pariin. Tosin on muistettava NSA:n ja NAC:n murtokykyisyys tämänkin tekniikan kohdalla. WPA2-turvatekniikan salasanan on oltava joukko numeroita ja/tai kirjaimia. Aivan kuten kaikkien muidenkin tekniikoiden salasanojen tulee olla. Heikko ja mahdollisesti jotain jollain kielellä tarkoittava sana tai looginen lause helpottaa hakkereiden työtä huomattavasti. (Spector 2011.)

Monia valmistajakohtaisia ratkaisuja WPA:n ja WPA2:n käyttöönoton helpottamiseksi on jo tarjolla. Nämä ratkaisut ovat tarkoitettu juuri hotspot-verkoissa vierailua yksinkertaistamaan. Tulevaisuudessa voidaankin odottaa virallista standardia IEEE:ltä, joka mahdollistaisi turvallisemmat verkkovierailut kaikkialla. (Cisco 2012.)

3 VPN

VPN (Virtual Private Network) tarjoaa huokean tavan turvallisiin verkkovierailuihin. VPN sallii tiedostojen jakamisen, videokonferenssit ja muut vastaavat palvelut. VPN-salausta käyttämällä ei kuitenkaan voi turvata esimerkiksi Skypellä soitettua verkkopuhelua, sillä Skype-palveluun liittyvät verkkopuhelut todettiin kevään 2013 aikana ilmenneiden paljastusten myötä epäluotettaviksi. Yhteys on salattu vain VPN-palvelimelle saakka, jonka jälkeen yhteys siirtyy Skypen palvelimelle. Tämän jälkeen yhteys on avoin Yhdysvaltain tiedustelupalvelulle. Vuoden takaiset paljastukset tosin viittaavat Microsoftin käyttöjärjestelmien sisältävän NSA:n takaportteja, joten tietoturvaa sopii aina epäillä. (Hyppönen 2013.)

VPN on myös käytössä lukuisten yritysten etäyhteyksissä. VPN toimii kaikissa nykyisissä älylaitteissa, kuten tableteissa ja uusissa älypuhelimissa. VPN-sovellus toimii myös kaikissa tunnetuimmissa käyttöjärjestelmissä. Tarvitaan vain toimiva VPN-asiakasohjelma, joka ottaa yhteyden VPN-palvelimeen. Dataliikenne on suojattua VPN-palvelimeen saakka, josta eteenpäin data jatkaa suojaamattomana. Käytännössä voidaan kuitenkin siirtää dataa anonyymisti, sillä VPN-palvelin piilottaa käyttäjän alkuperäisen IP-osoitteen. Näin ollen salakuuntelija ei pääse jäljittämään kuuntelemansa datan alkuperäistä lähdettä. (Mitchell 2013.)

VPN-tunneli turvaa langattomassa verkossa kulkevan datan. Käyttäjätunnukset ja salasanat ovat suojaamattomassa langattomassa verkossa vapaata riistaa hakkereille. VPN tunneli kuljettaa datan kryptattuna Internetin läpi haluttuun määränpäähän (end-point). Täysin murtamaton VPN tunneli ei kuitenkaan ole. Mikäli haetun datan määränpään palvelimet sijaitsevat esimerkiksi Yhdysvalloissa, ei luotettavuutta voida taata. Tämä johtuu Yhdysvaltojen mahdollisuudesta pakottaa palvelintarjoajia tallentamaan tiedonkulkua palvelimillaan. (ElitheComputerGuy 2013.)

VPN-tunnelissa käyttäjä on suojattu huijauksien tai salakuuntelun kaltaisilta hyökkäyksiltä, koska VPN-tunneli on luotu laitteessa olevan applikaation ja VPN-reitittimen välille. Niiden väliseen liikenteeseen eivät verkkosnifferit pääse pahantekoon. Verkkosnifferit ovat salasanoja etsiviä vakoiluohjelmia. Esimerkiksi Wireshark vakoiluohjelmalla voi haistella verkkoliikennettä. (ElitheComputerGuy 2013.)

VPN-perustyyppejä on kaksi. Yksi toimii OSI-mallin toisella tasolla ja toinen OSI-mallin kolmannella tasolla. OSI-mallin toisella tasolla toimiessa voidaan luoda virtuaalisia verkkokytkentöjä joiden välille muodostetaan virtuaalinen lähiverkko (VPN). OSI-mallin kolmannella tasolla, eli verkkokerroksella, toimiva VPN-yhteys voi hyödyntää erilaisia verkkotyyppejä, kuten X.25, NetWare IPX tai TCP/IP. Käytännössä kuitenkin hyödynnetään pääasiassa TCP/IP verkoista suurinta, eli internetiä. Siirto voi myös tapahtua UDP:llä. (Held 2004.)

3.1 VPN-protokollat

Toisen tason, eli OSI-mallin siirtoyhteyskerroksella, käytetään erilaisia tunnelointiprotokollia. PPP, eli Point-to-Point Protocol, on toiminut perustana nykyään käytetyille tekniikoille. PPTP, eli Point-to-Point Tunneling Protocol, kehitettiin PPP-pakettien lähettämiseen IP-verkon yli muodostaen asiakaspäätteen ja palvelimen välille VPN-yhteyden. (Held 2004.)

Layer Two Forwarding (L2F) on tunnelointiprotokolla, joka PPTP:n tapaan paketoi PPP-paketteja IP-verkon yli lähettämiseen. Layer Two Tunneling Protocol (L2TP) on käytännössä korvannut L2F:n. L2TP yhdistää tekniikoita PPTP:stä ja L2F:stä. L2TP käyttää UDP:tä siirrossa, jättäen virheentarkistuksen korkeamman tason protokollille. (Held 2004.)

Korkeamman tason VPN:n protokollia on useita. Mainitsemisen arvoisia ovat IPSec ja SSL. IPSec voidaan yhdistää L2TP-protokollaan, joka ei itsessään sisällä salausta. IPSec:in käyttöönotto on SSL:ää työläämpää. Molemmat tekniikat tukevat useita salausalgoritmejä ja tarkistussummia. (Held 2004.)

Secure Sockets Layer (SSL) on alunperin Netscape Communications Corporationin kehittämä tekniikka. SSL asettuu kolmannen ja neljännen OSI-mallitason väliin suojaten korkeamman protokollan yhteydet. Helposti käyttöönotettavana tekniikkana SSL:ää käytetäänkin yleisesti HTTP-yhteyksien suojaamiseen. SSL tukee sertifikaattien käyttöä ja Netilla Security Platformin avulla voidaan luoda yksinkertainen VPN:ä. Koska SSL-tuki löytyy useimmista selaimista, voidaan suojattuja yhteyksiä luoda ilman lisäohjelmien asennusta. (Held 2004.)

3.2 VPN-asiakasohjelma

Yksityishenkilöt ovat VPN-tunneloinnin väliinputoajia. Yritysmaailmassa VPN on kasvanut itsestään selväksi käytännöksi työntekijöiden etäyhteyksissä. Asiakasohjelman usein vaikea konfiguraatio sujuu yrityksen tietohallinnolta helposti, mutta yksityiskäyttäjillä tätä palvelua ei ole käytettävissä. (Perlmutter & Zarkower 2001.)

Ilmaisia VPN-asiakasohjelmia on tarjolla useita, mutta näiden olemassaolosta harvemmin muut kuin IT-taustaiset henkilöt ovat tietoisia. Sopivaa VPN-asiakasohjelmaa etsiessä voi maallikko vahingossa osua täysin vääränlaiseen ohjelmaan. Pahimmillaan jopa pahantahtoisen tahon ylläpitämään vakoiluohjelmaan, eikä maallikko osaa vaatia kolmannen osapuolen myöntämiä varmenteita. (Järvinen, P. 2003.)

Eräs turvallinen ja helppokäyttöinen VPN-asiakasohjelma on OpenVPN Client. OpenVPN toimii kryptattuna OSI-mallin toisessa tai kolmannessa kerroksessa käyttäen SSL-protokollaa. Open-

VPN tukee joustavasti käyttäjän varmennustekniikoita perustuen vahvistettuihin sertifikaatteihin. (OpenVPN Technologies 2013.)

Kuva 1: OpenVPN Client

VPN-asiakasohjelman käyttöönoton lisäksi tarvitaan VPN-palvelin, johon turvallinen yhteys muodostetaan. Yritysmaailmassa voidaan käyttää olemassa olevaa kalustoa josta VPN-palvelinominaisuus löytyy, kuten esimerkiksi palomuuri, reititin tai UTM-laite (Unified Threat Management). Ohjelmallinen VPN-palvelin onnistuu myös asentamalla sopiva ohjelmisto tehtävään soveltuvalle palvelimelle. Yksityishenkilö voi ottaa käyttöön kaupallisen palvelun, jolloin verkkonopeudessa ei yleensä huomaa muutosta. Vaihtoehtoisesti tarjolla on ilmaispalveluja, mutta nämä harvemmin kykenevät tarjoamaan riittäviä yhteysnopeuksia, eikä tietoturvasta ole takeita.

3.3 VPN-palvelin

Etäyhteydet reititetään VPN-palvelimen kautta yrityksissä yleensä paikalliseen sisäverkkoon. Yleisimmin yhteyden tarkoitus on muodostaa suojattu yhteys työntekijälle, jonka kautta hän voi toimia yritysverkossa aivan kuin olisi fyysisesti läsnä toimistossa (Perlmutter & Zarkower 2001). Yksityishenkilöille sen sijaan tarjotaan maksua vastaan VPN-reitityspalveluja, joiden avulla käyttäjän yhteys suojataan aina VPN-palveluntarjoajan internetiin yhdistävälle palve-

limelle saakka. Nämä palvelut on tuotteistettu kohtalaisen helppokäyttöisiksi. Hotspotshieldin VPN-palvelu on käyttäjilleen yksinkertainen asentaa ja ottaa käyttöön (Anchorfree 2013).

OpenVPN-ohjelmistoon puolestaan on yksinkertaista yhdistää Privatetunnelin VPN-palvelu (OpenVPN Technologies 2013). Kumpaakin palvelua voi kokeilla ilmaiseksi, mutta käyttöönottokynnys on edelleen monelle liian korkea. Kustannukset ja käyttäjän oma tietoisuus hänelle riittävästä tietoturvatasosta eivät ole yleisesti käyttäjien tiedossa. Yksityishenkilöt voivat myös yhdistää ilmaisiin VPN-palvelimiin, joita internetissä on useampiakin. Tässä on kuitenkin huomioitava se, että palvelua tarjoava instanssi ei välttämättä ole täysin luotettava ja yhteys VPN-palvelimesta internetiin voi olla hyvinkin hidas.

Laitetasolla VPN-palvelimena voidaan käyttää perinteisiä palvelinratkaisuja joihin on asennettu sopiva VPN-reititysohjelma. Useilta verkkolaitevalmistajilta on saatavissa dedikoituja VPN-laiteratkaisuja, jotka ovat helposti yhdistettävissä yritysten olemassa oleviin verkkokokonaisuuksiin. (Perlmutter & Zarkower 2001.)

Monesti palomuuriin sisältyy VPN-toiminnallisuus, jonka käyttöönotto on tietohallinnolle yksinkertainen tehtävä. Myös VPN-toiminnallisuuksin höystettyjä UTM-ratkaisuja (Unified Threat Management) on tarjolla useammalta laitevalmistajalta. (Perlmutter 2001.) Tärkeää on kuitenkin muistaa luoda käyttöönottosuunnitelma ja päivittää yrityksen tietoturva- ja tietoliikennepolitiikka jotta uusi ominaisuus saadaan hallitusti työntekijöiden käyttöön. (Allen 2002.)

PfSensen palomuuritekniikka mahdollistaa selkeän säännöstön hotspot-verkoille. Tämä auttaa pitämään reitittimen IP-taulun puhtaana. Näin reititin ei kuormitu ja reitittimen toiminta pysyy vakaana. Ruuhkaisina sisäänkirjautumisaikoina pfSensen ”per-rule” tekniikkaa hyödyntämällä käyttäjämäärää voi rajoittaa tai hidastaa. (Electric Sheep Fencing LLC 2013.)

Pienverkoille tarkoitettuja dedikoituja VPN-palvelimia ei toistaiseksi ole tarjolla useita. Sen sijaan yhä useammin kuluttajille ja pientoimistoille tarkoitettu reititin omaa VPN-palvelintoiminnon. Olemassa oleviin pienverkkoreitittimiin voi myös halutessaan asentaa esimerkiksi Linuxiin pohjautuvan DD-WRT-laiteohjelmiston, joka korvaa valmistajan alkuperäisen laiteohjelmiston ja mitätöi takuun. DD-WRT tarjoaa erittäin laajan kirjon toiminnallisuuksia, joista VPN-palvelintoiminto on yksi. (DD-WRT 2014.)

3.4 Sertifikaatit

VPN-yhteyden osapuolet tunnistaakseen luotettavasti, on käytettävä sertifikaatteja eli varmenteita. Sertifikaatti on sähköinen todistus, jonka myöntää kolmas osapuoli. Sertifikaatin myöntäjän on tietenkin oltava tunnettu ja luotettava taho. (Järvinen, P. 2003.)

Sertifikaatti voi olla organisaation sisäinen tai se voi olla ostettu palvelu. Yleisin sertifikaatin käyttö-tapahtuma on HTTPS-yhteyden muodostus, jossa TLS-pohjainen suojaus varmennetaan. Käyttäjä harvemmin huomaa varmennustapahtumaa, ellei palveluntarjoaja ole unohtanut uusia sertifikaattia, jolloin selain antaa varoituksen tästä. Sertifikaattien voimassaoloaika on palveluntarjoajan päätettävissä, mutta jos kyse on maksullisesta palvelusta voi sertifikaatin validiteetti raueta maksu-suorituksen unohtamisesta. (Strebe 2004.)

Käytännössä sertifikaatti on digitaalinen allekirjoitus, joka puolestaan on luotetun osapuolen allekirjoittama. Allekirjoitukset ovat tarkistussummia, eli tiivistelmälaskuja alkuperäisestä datasta. Allekirjoitukset ovat salattuja. Salaus puretaan julkisella avaimella ja verrataan myöntäjän palvelussa (CA, Certificate Authority) oleviin tietoihin. Tietojen täsmätessä on luotettavuus varmistettu. (Strebe 2004.)

3.5 Tietoturvallisuus

Tietokirjailija Petteri Järvinen esittää kirjassaan Salausmenetelmät kysymyksen, joka on käynyt monen yksityishenkilön mielessä: ”Kuka nyt minun viestejäni lukisi?”. Yksityisen käyttäjän kannalta merkityksettömältä vaikuttava tieto voi väärissä käsissä olla hyvinkin arvokasta. (Järvinen, P. 2003.) Riskit ovat todellisia ja tiedon salakuuntelun uhriksi voi joutua kuka vain. Vahingon suuruuden määrittelee hakkerille vuotaneen tiedon arvo. Julkisessa verkossa kuljetettu tieto kulkee salattuna virtuaalisen verkon avulla. VPN-WLAN-tietoturvasovellus salaa tiedot VPN-tunneleiden avulla. Vain sallitut käyttäjät pääsevät VPN-tunneliverkon piiriin, jolloin julkisesta verkosta saadaan jokaiselle käyttäjälle oma salattu virtuaalinen kaistansa. VPN-palvelimen kapasiteetista riippuu virtuaalisten kaistojen määrä. (Spamlaws 2013.)

Verkossa tietoa, eli dataa, voidaan salakuunnella. Tämä data saattaa olla merkityksetöntä ja toisinaan on jopa toivottavaa, että tieto vuotaisi julkisuuteen. Tietovuodoista otettakoon esimerkiksi näytönohjaimia valmistavien yritysten läpinäkyvä toiminta. Kuluttajien kiinnostus pidetään yllä vuotamalla ”salaista tietoa” tulevista laiteparannuksista. Lähes aina verkossa surffailuun liittyy kuitenkin henkilökohtaisten tunnusten käyttöä. Nämä käyttäjätunnukset, salasanat ja muu informaatio ovat käyttäjilleen arvokasta tietoa. On muistettava, että ne ovat myös todella arvokasta tietoa myös verkkosniffereille. (Järvinen, P. 2003.)

Verkkosnifferit etsivät järjestelmällisesti dataa, jota sitten käyttävät omiin tarkoituksiinsa. Säilyttääkseen luottamuksellisuutensa on data suojattava. Käyttäjien verkkovierailut voidaan suojata monin eri tavoin. Tavallisimpiin tekniikoihin kuuluu salatut HTTPS-yhteydet. Varsinkin palveluihin kirjautuessaan käyttäjäkohtaiset tunnistustiedot siirretään salattuja tiedonsiirtoprotokollia hyväksikäyttäen. Ikävä kyllä, moni palvelu siirtää kirjautumistiedot edelleen sa-

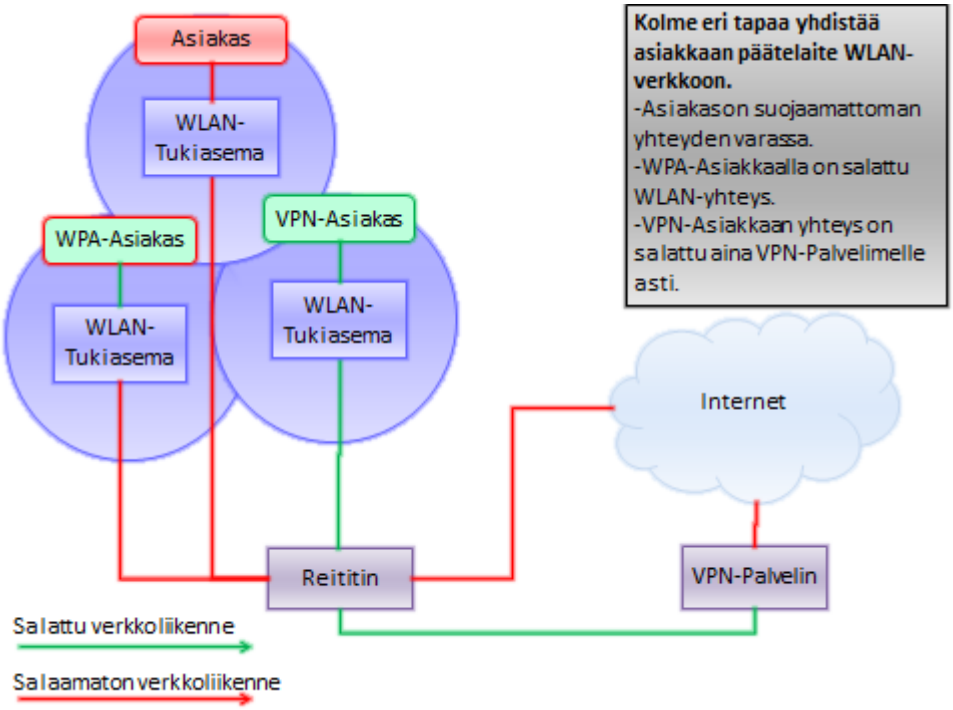
laamattomana verkon yli. Haitallisen tahon salakuunnellessa salaamatonta verkkoa kirjautumistietojen luottamuksellisuus menetetään (Järvinen 2003). VPN-WLAN-tietoturvasovelluksen käyttö vaikeuttaa salakuuntelua huomattavasti. Verkkoa ulkoapäin salakuunteleva taho saa käsiinsä vain kryptattua dataa. Salakuuntelija joutuisi murtautumaan fyysisesti NextMesh Internationalin palvelintiloihin päästäkseen VPN-verkkoon käsiksi. Käytännössä VPN WLAN tietoturvasovellus siis suojaa käyttäjän ulkoisilta uhilta täydellisesti.

Käytännössä urkkija voisi saada erittäin paljon vahinkoa aikaan esimerkiksi salakuuntelemalla liikennettä NextMesh Internationalin hotspot-verkossa. Urkkijan saadessa esimerkiksi useita tuhansia nimiä yhdistettyinä aktiivisiin sähköposteihin, on näinkin yksinkertaisella paketilla iso arvo. Sähköposteista ja nimistä tai käyttäjänimistä koostuvan paketin voi myydä eniten tarjoavalle, tietoja väärinkäyttävälle taholle. Tämä epämääräinen taho voisi puolestaan käyttää kyseisiä osoitteita viruksen tai esimerkiksi rahanhuijausviestin levittämiseen. NextMesh Internationalin hotspot-verkossa urkkija voi WLAN-verkossa saada selville esimerkiksi käyttäjän nimen ja henkilötunnuksen sähköpostin tai Facebookin kautta. Näitä väärinkäyttämällä hän voisi esimerkiksi siirtää käyttäjän Kela-tuet liikkumaan jatkossa itse määräämälleen tilille.

4 WLAN:in suojaus VPN-tunneloinnilla

Seuraavilla sivuilla on kuvaukset VPN-WLAN-turvasovelluksen topologiasta. Kuvaukset selventävät salatun ja salaamattoman verkon liikennettä kohti Internetiä. Kuvauksissa huomioidaan salakuuntelijan väliintulo käyttäjän ja WLAN-tukiaseman välille.

Seuraavassa kuvassa havainnollistetaan NextMesh Internationalin tarjoamien langattomien verkkojen topologiaa. Kuvassa punaisella merkitty asiakas kuvaa verkon nykytilaa. Kuvaan on myös lisätty WPA-asiakas, joka puolestaan kuvaa langattoman verkon salaustekniikan tarjoamaa reittiä ja sen salatun liikenteen osuutta. VPN-asiakas on kuvassa ainoa, jonka liikenne pystyy tarjoamaan salauksen ja internetiin nähden anonymiteetin.



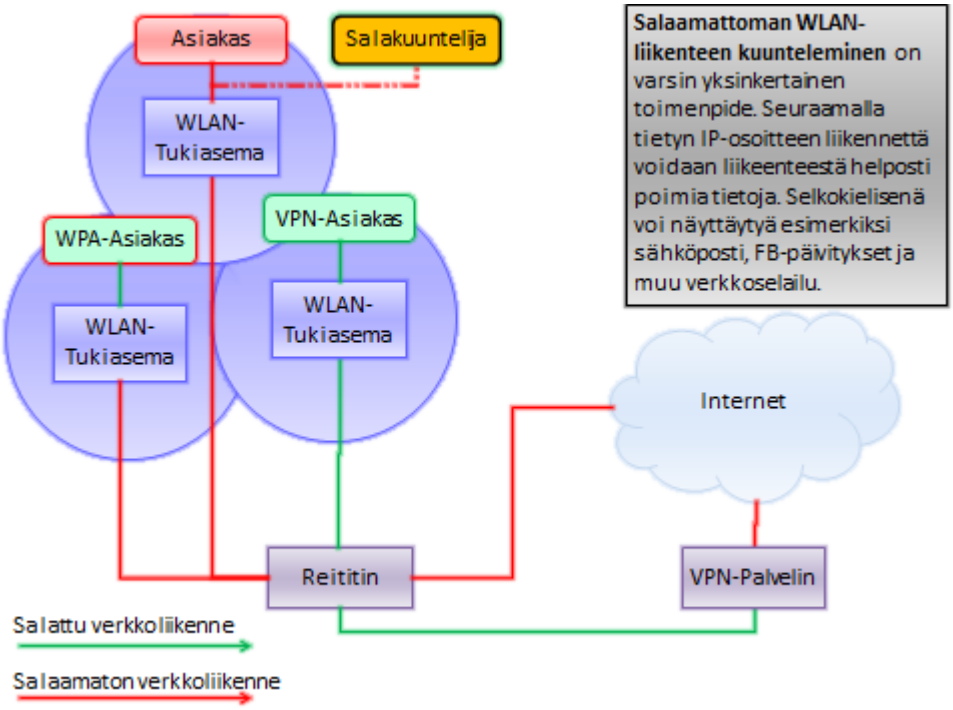
Kuva 2: WLAN-verkkotopologia

Seuraavassa kuvassa tarkastellaan salaamattoman langattoman verkkoliikenteen yksinkertaisinta tietoturvaongelmaa. Punaisella kuvattu Asiakas on yhdistänyt päätelaitteensa langattomasti avoimeen tukiasemaan. Asiakkaalla ei ole mahdollisuutta suojautua salakuuntelulta.

Kuvassa keltaisella merkitty Salakuuntelija voi tehtävään soveltuvalla ohjelmistolla seurata Asiakkaan langatonta verkkoliikennettä. Pahimmillaan Asiakkaan päätelaite tarjoaa käyttöjärjestelmän jakamia resursseja, kuten valokuvia ja dokumentteja, langattoman verkon muille käyttäjille.

NextMesh Internationalin langatonta hotspot verkkoa kokeiltiin kauppakeskus Isossa omenassa kahdella kannettavalla tietokoneella. Kannettavissa koneissa on Windows 7 käyttöjärjestelmät. Liikenteen seuraamista pystyttiin tekemään, vaikka langattoman verkon käyttäjät ovat toisistaan näennäisesti eristyksissä. Wireshark-vakoiluohjelman avulla keskinäistä liikenteenkulkua voitiin testikoneiden välillä kuunnella estotta. Muiden verkkoasiakkaiden liikennettä ei missään vaiheessa seurattu tai tallennettu, vaan kaikki verkkoliikennekuuntelu tapahtui testikoneiden kesken.

Langattoman verkkoliikenteen salakuuntelu osoittautui suhteellisen helpoksi. Internetissä on tarjolla monia tehtävään sopivia ohjelmistotyökaluja ja ohjeita. Tarjolla on niinkin erikoistuneita ohjelmia, kuin Facebookin salakuunteluun tarkoitettu internetselaimen lisäosa. Lisäosan asennus on niin yksinkertainen, että tavallinenkin käyttäjä selviäisi tehtävästä.

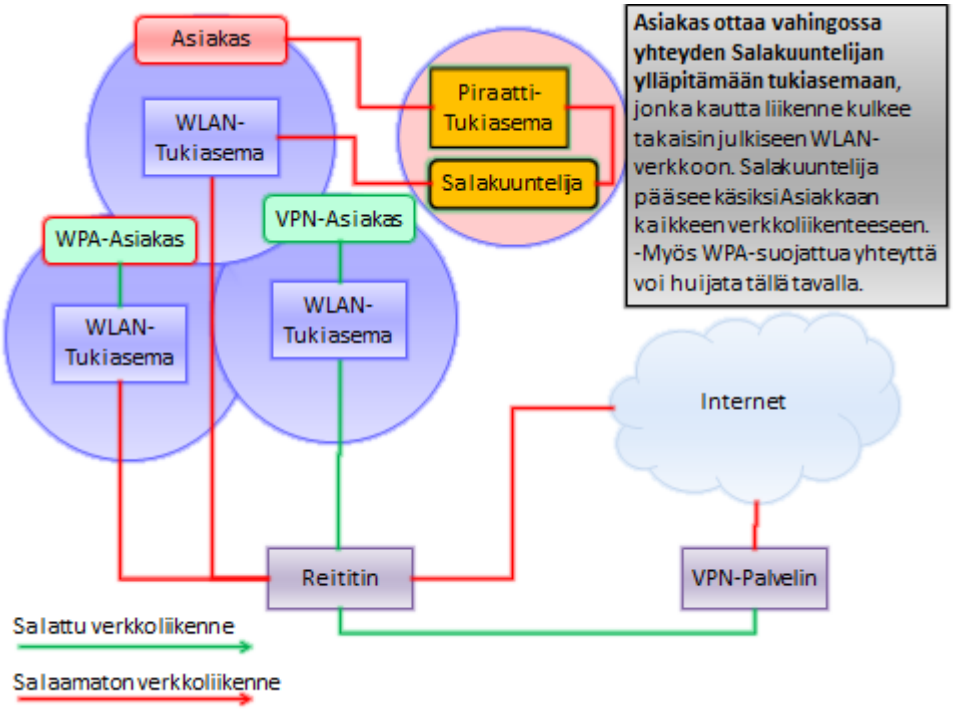


Kuva 3: Salaamattoman liikenteen kuuntelu

Useat internetissä tarjottavat palvelut tarjoavat HTTPS suojattuja yhteyksiä, jossa liikenne asiakkaalta verkkosivulle asti liikkuu salattuna. Esimerkiksi verkkopankit käyttävät tätä hyväkseen. Facebook tarjoaa myös mahdollisuuden yhteyden salaamiseen tällä tekniikalla, mutta se on erikseen kytkettävä päälle Facebookin asetussivulta.

Täysin turvassa ei pelkällä HTTPS:yhteydellä ole yksikään salaamatonta WLAN-yhteyttä käyttävä. Mikäli päätelaitteen tietoturva-asetukset palomuuria ja tiedostonjakoa myöten eivät ole kunnossa on salakuuntelijan helppo urkkia päätelaitteeseen tallennettuja tiedostoja ja mahdollisesti myös aiheuttaa ohjelmallisesti haittaa laitteelle.

Seuraava kuva esittää klassisen ”man-in-the-middle”-salakuuntelutilanteen. Esittämällä luotettavaa WLAN-tukiasemaa voi salakuuntelija päästä käsiksi Asiakkaan verkkoliikenteeseen, vaikka liikenne olisikin suojattu WLAN:in tarjoamin tekniikoin.



Kuva 4: Tukiasemahuijaus

Asettamalla oman tukiaseman SSID:n, eli langattoman verkkotunnuksen, tunnetun salasanan ja salaustekniikan (WEP/WPA/WPA2) samaksi, kuin yleensä luotetun paikallisen WLAN-verkon, on salakuuntelijalla helppo pääsy tukiaseman asiakkaiden verkkoliikenteeseen. Tällaisen huijauksen voi liian helposti luoda kannettavalla tietokoneella esimerkiksi kauppakeskuksen parkkihalliin pysäköityyn autoon. Tämä ajatusleikki perustuu Bartzin 2012 opetuksiin WEP, WPA ja WPA2 salaustekniikoista, joita käsiteltiin luvussa 2.4.

WLAN-verkon salaus on voimassa vain päätelaitteen ja tukiaseman välillä. Salakuuntelija voi helposti seurata tukiaseman edelleen reitittämää salaamatonta liikennettä. Asiakkaan verkkoliikenne reititetään internetin suuntaan käyttäen aitoa paikallista WLAN-verkkoa tai vaikkapa 3G- tai 4G-yhteydellä.

WPA- ja WEP-salaukset sisältävät tunnettuja haavoittuvuuksia. Näitä vanhempia salaustekniikoita kannattaa tämän vuoksi välttää, elleivät yhteensopivuusongelmat vanhempien päätelaitteiden kanssa ole este. Tällä hetkellä WPA2-suojattu langaton verkko on paras WLAN-suojaus. WPA2 ei myöskään ole täydellinen ja sisältää haavoittuvuuksia, mutta tarjoaa varsinkin kotikäytössä melko luotettavan suojan.

Turvallisimpana ratkaisuna voidaan pitää VPN-yhteyttä, joka salaa verkkoliikenteen aina VPN-palvelimelle saakka. VPN-palvelin voi sijaita lähiverkon laidalla palomuurin suojassa, jolloin salakuunteluyritykset lähietäisyydeltä epäonnistuvat.

Suojattuja VPN-yhteyksiä tarjotaan myös ostettavina palveluina internetissä. Pääteohjelma luo tällöin suojatun yhteyden asiakaslaitteelta lähiverkon ja internetin yli aina palveluntarjoajan palvelimelle asti. Tällöin saavutetaan anonymiteetti, palveluntarjoajan maan lakikäytännöistä riippuen, joka ei paljasta edes käyttäjän alkuperämaata. Tällaiset yhteydet tosin kärsivät usein hitaudesta, joka johtuu pitkistä yhteyksistä verkkojen yli ja palveluntarjoajan palvelin- ja yhteyskapasiteetista.

4.1 NextMesh International verkkoasiakas

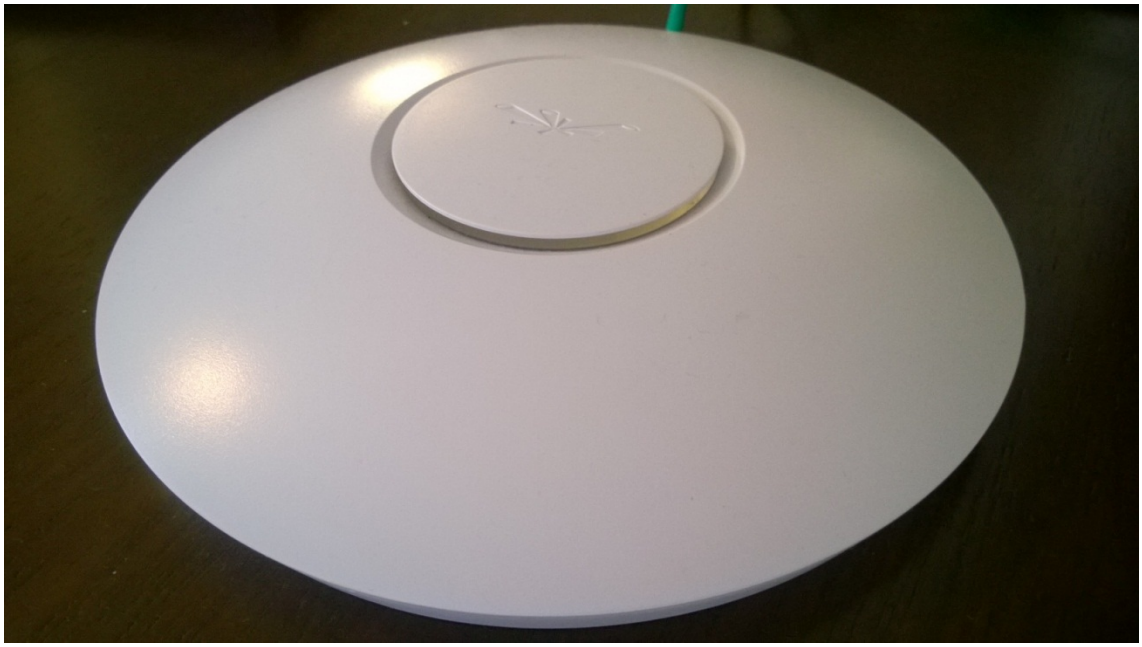
NextMesh Internationalin hotspot-verkkojen asiakkaiden päätelaitteet voivat vaihdella hyvinkin paljon. Päätelaitteena voi toimia yhtä hyvin puhelin, tabletti kuin kannettava tietokonekin. Monesta puhelimesta toki löytyy mobiilidataliittymä, mutta harvemmin kannettavasta tietokoneesta tai tabletista. Mobiilidataliittymästä huolimatta WLAN-verkon käyttö on houkuttelevaa tämän tarjotessa huomattavasti nopeamman verkkoyhteyden. (Järvinen, M. 2013.)

NextMesh Internationalin ylläpitämä verkko tarjoaa uuden kanavan paikallisille kaupallisille toimijoille olla yhteydessä kuluttajiin. Yhdistäessä WLAN-verkkoon päätelaitteen selain ohjataan NextMesh Internationalin luomalle aloitussivulle, jolta voi ostaa mainostilaa. WLAN-verkon asiakas lunastaa itselleen puolen tunnin verran käyttöaikaa klikkaamalla mainosta. (NextMesh International 2013.)

WLAN-verkon internetyhteys on ohjelmallisesti jaettu käyttäjien kesken niin, että yksi käyttäjä ei voi varata koko internetkaistaa itselleen. Käytännön kokeet Isossa Omenassa kesäkuussa 2013 osoittivat, että järjestelmä kuormantasaajaa myöten toimii luotettavasti. Myös internetyhteys on riittävän nopea jopa täyden teräväpiirtovideon katseluun (Youtube, 1080p).

4.2 WLAN-tukiasema

Tukiasemat toistavat ja vahvistavat signaaleja. Tukiasemia käytetään keskittimien, kytkimien ja reitittimien kanssa tukemaan langallisia tai langattomia verkkoja. Tukiaseman lähettämät signaalit ovat langattomia ja erittäin tarpeellisia, jotta saadaan muun muassa isot toimitilat katettua langattoman verkon piiriin. Tukiasema on liitettävä reitittimeen, jotta saadaan kattavat signaalit Internet-yhteyteen. Käyttäjän muodostaessa yhteyttä julkiseen langattomaan verkkoon, hän käyttää yleensä tukiasemaa. Reititin voi myös itsessään olla tukiasema, tällöin kyseessä on kuitenkin kotikäyttöön tarkoitettu laite. (Microsoft 2013.)



Kuva 5: NextMesh International Oy:n käyttämä Ubiquitin tukiasema

Yleensä tukiasema yhdistetään reitittimeen, jonka kautta muodostetaan yhteys lähiverkkoon. Uudemmat yrityksille suunnatut tukiasemat käyttävät PoE-tekniikkaa (Power over Ethernet), jolloin tukiasemaan saadaan virta ethernetkaapelin kautta ja kaapelisotku vähenee. Kotikäyttöön suunnatut reitittimet eroavat suuresti yrityksille suunnatuista laitteista ominaisuuksiltaan. Yrityskäyttöiset tukiasemat kustantavat useita satoja euroja, kun taas kotikäyttöön suunnattujen laitteiden lähtöhinta on muutamia kymppejä. (Verkkokauppa.com 2013.)

Tukiasemassa on oltava riittävät ominaisuudet etähallinnan osalta yrityskäytössä, kotikäytössä tätä tukea ei vaadita. Tukiaseman tärkeimpiä ominaisuuksia ovat yleiset salaustekniikat, lähinnä WPA2, ja yrityskäytössä 802.11x-suojaustekniikka. Yhdistettynä suojattuun VPN-WLAN-tietoturvasovellukseen pystytään luomaan riittävä suoja salakuuntelua vastaan. (Bartz 2012.)

4.3 Reititin

Reitittimet mahdollistavat tietoliikenteen kulun verkossa. Kaikkien verkossa toimivien laitteiden, kuten älypuhelinten, tablettien ja tietokoneiden toiminta Internetiin saadaan aikaiseksi reitittimien avulla. Reitittimet ohjaavat verkon liikennettä ja ne ovat joko langallisia tai langattomia. (Microsoft 2013.)

Kuva 6: Reititin NextMesh International Oy

PfSense-ohjelmisto on päävastuussa kaikkien IP-osoitteiden jakamisesta. Reititin hakee pfSensen tiedoista vapaan IP-osoitteen asiakkaan istuntovierailun ajaksi DHCP-protokollan avulla. PfSensen ominaisuuksiin kuuluu myös rajausmahdollisuus käyttöjärjestelmiä koskien. Minkä tahansa yksittäisen käyttöjärjestelmän voi rajata pfSensen avulla, jolloin voidaan toteuttaa käyttöjärjestelmäkohtaisia palveluita. PfSense hyödyntää edellä mainitussa pOf-järjestelmää, eli passiivista ja kehittynyttä käyttöjärjestelmän ja verkon tunnistusmallia, jolloin voidaan esimerkiksi rajata kaikki muut käyttöjärjestelmää käyttävät laitteet sovelluksen ulkopuolelle lukuun ottamatta Android-käyttöjärjestelmää. (Electric Sheep Fencing LLC 2013.)

NAT, eli osoitteenmuutos on myös tärkeä osa reitittimen toimintaa. NAT-tekniikka reitittää lähiverkon liikenteen yhden IP-osoitteen kautta ulos. Näin ollen tarvitaan vain yksi julkinen IP-osoite reitittimelle, joka jaetaan kaikkien julkista hotspot-verkkoa käyttävien laitteiden kesken. NAT-tekniikan hieman jäykkien säädösten vuoksi NAT aiheuttaa ongelmia muun muassa IPSec-turvaprotokollan kanssa. NAT-tekniikka on jäykkyydestään huolimatta Ciscon GRE tekniikkaa luotettavampi hotspot-verkkoja varten. (Salmenkylä 2012.)

5 Verkkosuojausten testaus

Langattomien verkkojen suojausten testaus todistaa kuinka helposti määrätietoinen hakkeri kykenee murtamaan useimmat suojaukset. Kyseessä on nimenomaan langattoman verkon kautta tapahtuva tietomurto. Langallisen verkon salakuuntelu vaatisi kohteen julkisen IP-osoitteen tuntemisen, joka on usein palveluntarjoajan dynaamisesti asettama. Dynaaminen IP vaihtuu jokaisella yhteyskerralla, jolloin kohteen löytäminen on erittäin haastavaa.

Kuten teoriaosuuden kappaleessa (2.4) todettiin, WPA2 on tätä kirjoitettaessa WLAN-verkkojen vahvin suojaus. Seuraava suojausmuuri tulee vastaan vasta HTTPS-protokollan muodossa. Näiden kahden suojauksen turvallisuuden vaillinaisuus haluttiin todistaa kokeellisesti.

Tulevaisuudessa IPv6:n mukanaan tuoma IPSec-suojaus tulee lisäämään salakuuntelun vaikeutta huomattavasti. Ikävä kyllä, IPv6 antaa odottaa läpimurtoaan vielä pitkään. IPv4:n kanssa voidaan käyttää IPSec-suojausta, mutta tämän käyttöönotto vaatii asiantuntemusta. Myös laitteiston yhteensopivuus on kyseenalaista käytettäessä IPSec:ia IPv4:n yhteydessä.

5.1 Langattoman verkon suojauksen murtaminen

Koemielessä testasimme turvallisimman WLAN-salauksen, eli WPA2:n, murtamista. Salaukseen käytetään 256-bittistä avainta, jonka murtaminen raa'alla laskentavoimalla veisi tavalliselta PC-tietokoneelta useita päiviä. Koska langattomiin verkkoihin liitetään useita laitteita, olisi esimerkiksi kodissa epäkäytännöllistä käyttää vaikeasti muistettavaa salasanaa. Perheenjäsenten ja vieraiden yhdistäessään kannettavia tietokoneitaan ja älypuhelimiaan verkkoon, pitäisi kaivaa esille lunttilappu, joka muistuttaisi siitä, että salasana on ”GrX40Ff155Rt”.

Usein salasanana käytetään sanaa, jonka koko perhe muistaa helposti. Lemmikkieläimet, sukunimi tai verkon nimi ovat helppoja muistaa. Verkkopalveluiden salasanamurrot ovat useaan kertaan todistaneet ihmisten laiskuutta salasanojen hallinnassa. Tästä syystä tehokkain tapa murtaa WLAN-verkon salaus on sanakirjahyökkäys.

Sanakirjahyökkäyksessä kokeillaan tiedostoon tai tietokantaan tallennettuja sanoja vuoronperään toivossa, että jokin vastaisi salasanaa. Tähän hyökkäykseen voidaan melko helposti yhdistää pienten ja ison kirjainten kokeilu tai 1337, jossa kirjaimet on korvattu numeroin. Tavalliset sana-numero yhdistelmät voidaan myös kokeilla, esimerkiksi Salasana123.

Kuva 7: Salasanan pituuden vaikutus murtoaikaan

Salauksen murtamiseen tarvittava aika kasvaa eksponentiaalisesti salasanan pituuden myötä. Sanakirjahyökkäystä käytettäessä jokainen selvään sanaan lisätty muutos ainoastaan kaksinkertaistaa murtamiseen tarvittavan ajan.

5.2 WLAN-verkkoon murtautuminen käytännössä

Kokeilimme WPA2-suojattuun verkkoon murtautumista salasanahyökkäyksellä. Windowsin laiteajureiden rajoitusten vuoksi oli siirryttävä Linuxin puolelle. Wireshark, jota suosimme paljon testauksessa, on onneksi tarjolla molemmille käyttöjärjestelmille.
Kali-Linux on julkaisu, joka on suunniteltu verkkotestaukseen. Mukaan oli paketoitu useita hyviä työkaluja ja asennus USB-tikulle oli nopeasti suoritettu. Kalin käynnistymisen jälkeen laiteajurit ladattiin verkkokortille (Intel N6205) ja toiminta saatettiin aloittaa.
Windowsin puolella suurin ongelma oli verkkokortin saaminen tilaan, jossa kuunneltiin yhtä verkkoa aiheuttamatta omaa liikennettä. Tämän suorittaminen Kali-Linuxissa oli Wiresharkissa muutaman ruksin takana asetuksissa. Komentoriviltäkin toiminto saatiin helposti käyttöön. Airmon-ng on ohjelma, jolla saatoimme verkkokortin tilaan, jossa pystyttiin kuuntelemaan kohdeverkon liikennettä huomaamattomasti.

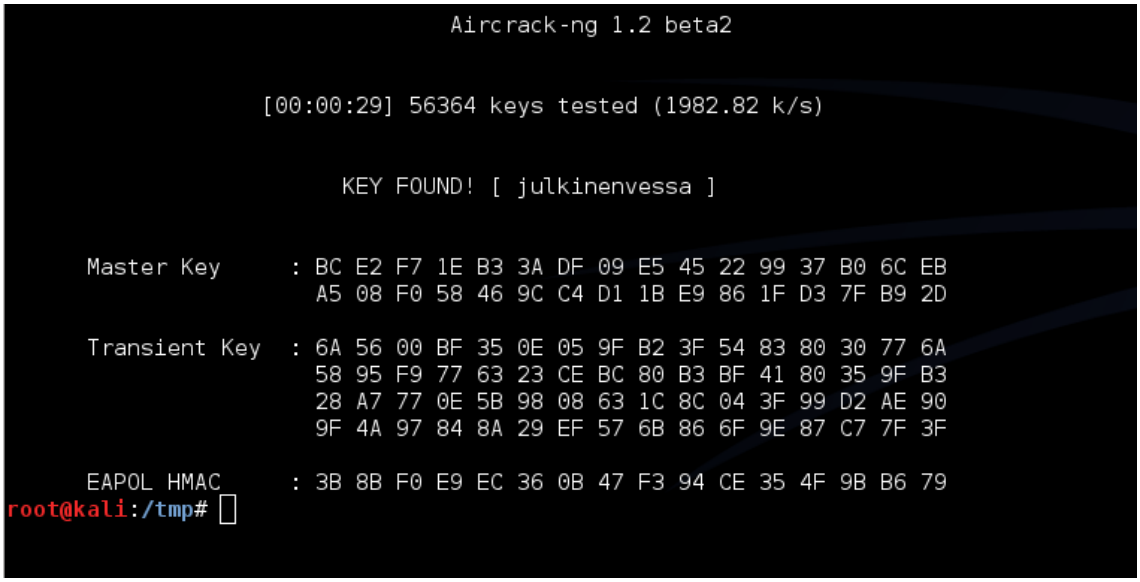
```
root@kali:~# sudo airmon-ng start wlan0


Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID     Name
3107    NetworkManager
3218    wpa_supplicant
3904    dhclient
Process with PID 3904 (dhclient) is running on interface wlan0


Interface       Chipset         Driver

wlan0           Intel 6205      iwlwifi - [phy0]
                                (monitor mode enabled on mon0)
```

Kuva 8: Airmon-ng salakuunteluohjelma

```
root@kali:~# sudo airodump-ng mon0


 CH  8 ][ Elapsed: 12 s ][ 2014-02-10 17:14 ][ WPA handshake: CC:5D:4E:29:5E:9C

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 0E:27:22:F9:03:85  -39       38        0    0  11  54e. WPA2 CCMP   PSK
 CC:5D:4E:29:5E:9C  -35       49       43    0   9  54e. WPA2 CCMP   PSK
 0A:27:22:F9:03:85  -47       46        0    0  11  54e. WPA2 CCMP   PSK
 06:27:22:F9:03:85  -44       36        0    0  11  54e. OPN
 00:24:A5:34:05:2A  -67       26        0    0   4  54e. WPA2 CCMP   PSK
 08:60:6E:5F:0D:F4  -68       17        1    0   1  54e  WPA2 CCMP   PSK
 50:67:F0:32:3A:19  -75        7        0    0  13  54e  WPA2 CCMP   PSK
 08:76:FF:95:92:CA  -79       15        0    0   8  54e  WPA2 CCMP   PSK
 08:76:FF:82:C7:A4  -82       11        0    0   6  54e  WPA2 CCMP   PSK
 B0:C7:45:14:0C:98  -85        8        0    0  11  54e. WPA2 CCMP   PSK
 54:E6:FC:35:72:A4  -84       11        0    0   6  54 . WPA2 CCMP   PSK
 00:1D:73:B2:77:59  -87       12        0    0   9  54e. WPA2 CCMP   PSK
 00:24:A5:B6:07:25  -87        4        0    0   6  54e  WPA2 CCMP   PSK
 08:60:6E:E0:81:80  -87        2        0    0   6  54e  WPA2 CCMP   PSK
 34:08:04:BF:1E:CE  -87       11        0    0  13  54e  WPA2 CCMP   PSK
 00:24:A5:34:4A:26  -88        2        0    0  11  54e. WPA2 TKIP   PSK
 34:21:09:09:03:C4  -87        6        0    0   1  54e  WPA2 CCMP   PSK
 1C:BD:B9:B3:45:F0  -88        2        0    0   6  54e. WPA2 CCMP   PSK
```

Kuva 9: Langattomia verkkoja jotka Airmon-ng löysi testialueelta

Ensimmäiseksi SSID-nimet piilotettiin yksityisyyden suojaamiseksi. Seuraavaksi aloitettiin verkkoliikenteen tallennus tiedostoon. Airmon-ng osasi ilmoittaa kun verkkoliikennettä oli tallennettu tarvittava määrä salasanamurron suorittamiseen. Seuraamalla verkkoliikennettä ja poimimalla tästä tietyt toistuvat paketit on mahdollista poistaa salausprotokollan lisäämät osuudet jolloin jäljelle jää verkonhaltijan asettama salasana, joskin edelleen salattuna.

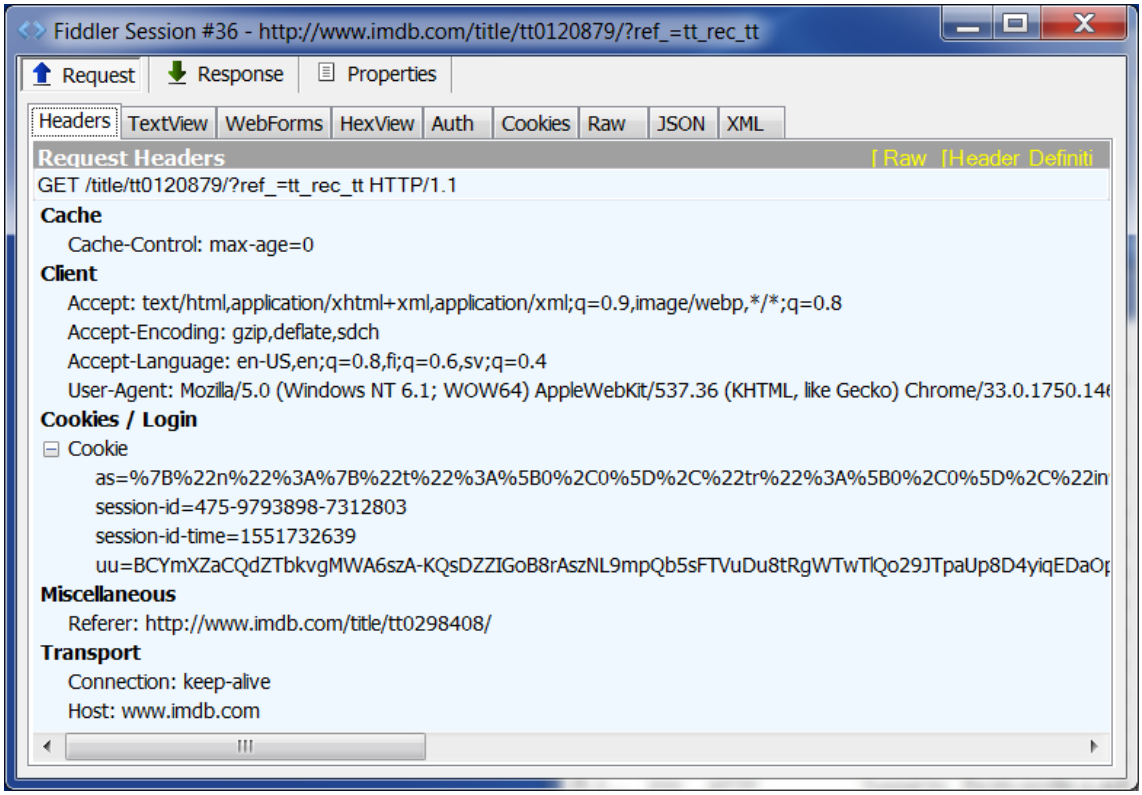


Kuva 10: Aircrack-ng on löytänyt verkon salasanan.

Aircrack-ng:llä aloitettiin salasanojen kokeilu kun verkkoliikennettä oli tallennettu tarvittava määrä. Sanakirjahyökkäys suoritettiin käyttäen OpenOffice.org:in suomenkielistä sanakirjaa, joka sisältää 359 000 sanaa. Sanoja kokeiltiin aakkosjärjestyksessä, jolloin sanakirjan keskivaiheille asettuva salasana löytyi puolessa minuutissa. Murtoon käytetty kannettava tietokone on laskuteholtaan hidas, mutta oikeilla työkaluilla reitittimen salasana selvisi 29 sekunnissa. Huomioitavaa on, että Aircrack-ng:n hakumääritykseen rajattiin suomenkieliset sanat.

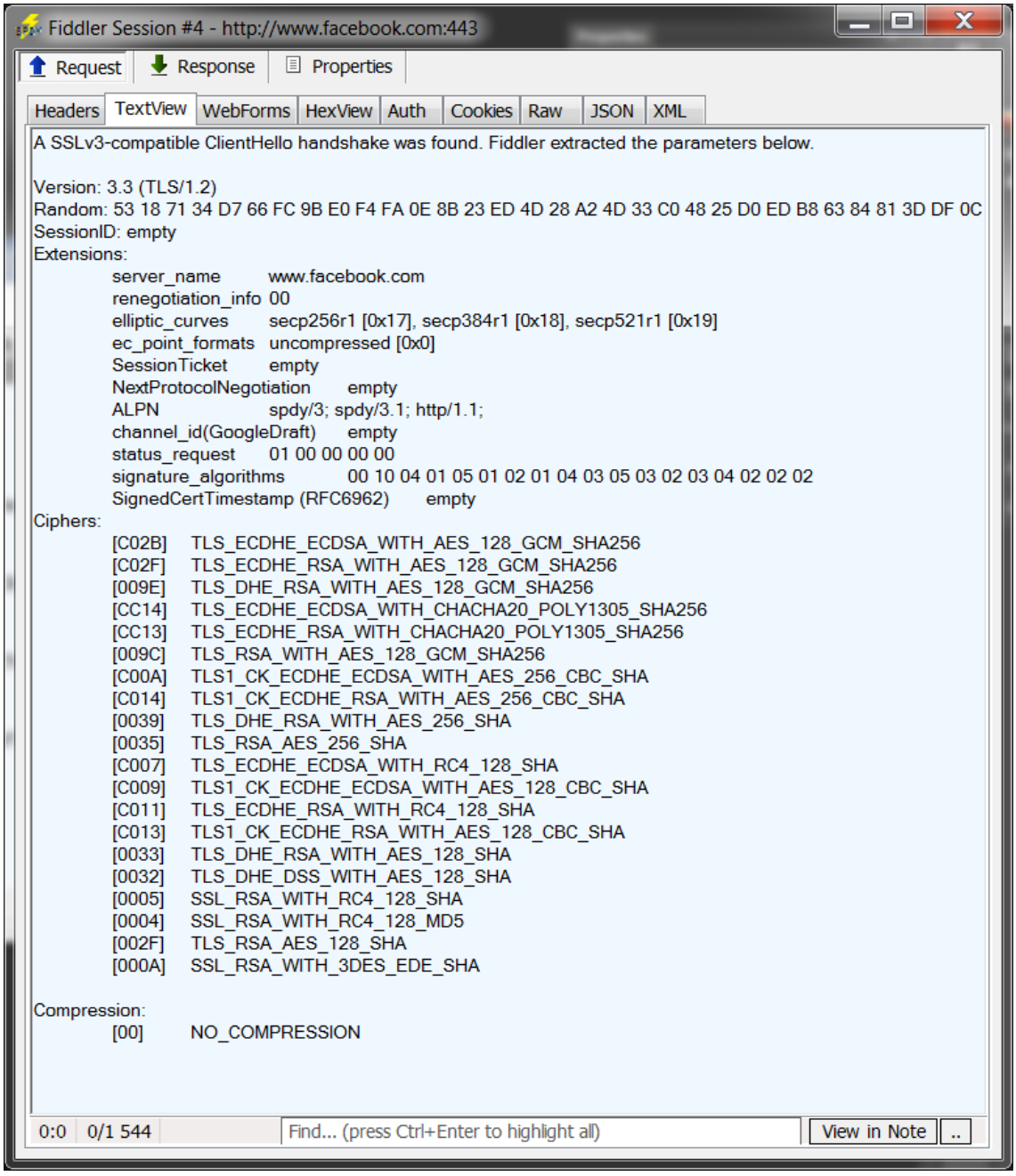
5.3 Verkkoliikenteen tulkinta

Vaikka verkkoliikenteen WPA2-salaus olisi purettu, on liikenteen tulkinta vaikeaa. Useat verkkotyökalut pystyvät kaappaamaan liikennettä, mutta esimerkiksi Wireshark ei osaa jakaa liikennettä kuin erillisiksi protokollapaketeiksi. Paketteja pystyy avaamaan, mutta tulkinta on vaikeaa, varsinkin kun lähetykset on jaettu useampaan pakettiin. Fiddler kuvassa on IMDB-verkkosivustoon luotu yhteys.



Kuva 11: Fiddler esittää HTTP-liikenteen tiedot helposti luettavassa muodossa

Fiddler on ilmainen työkalu, jolla varsinkin HTTP-paketit saadaan järjestykseen tulkinnan helpottamiseksi, jopa HTTPS-protokollan suojaamaa liikennettä on mahdollista salakuunnella. HTTPS-suojaus kierretään kaappaamalla asiakkaan ja palvelun välinen liikenne, jolloin Fiddler toimii näkymättömänä välikätenä. Fiddler paljastaa useita tietoja käytetystä salauksesta.



Kuva 12: HTTPS-yhteyden tiedot Facebookia käytettäessä

5.4 VPN-ohjelmistojen turvallisuus

Testauksen kautta pystyttiin toteamaan, että langattomassa verkossa tapahtuva liikenne ei ole turvassa salakuuntelulta. Viimeiseksi kokeiltiin liikenteen salausta NextMeshin käyttämällä OpenVPN-protokollalla. Liikenne salattiin asiakasohjelmalla ja kuljetettiin NextMeshin VPN-palvelimelle, joka sijaitsee yrityksen reitittimellä. Reititin purkaa ulospäin suuntautuvan liikenteen salauksen, josta liikenne jatkaa alkuperäisellä protokollalla internetiin. VPN-asiakkaan IP-osoite on suojassa, sillä internetin suuntaan näkyy vain NextMeshin reitittimen IP-osoite.

Testausta tehtiin käyttäen NextMeshin reititintä ja WLAN-tukiasemaa. Mielenkiintoista WLAN-tukiasemassa oli PoE-virransyöttö, eli Power Over Ethernet. Tässä laitteen tarvitsema virta syötetään ethernet-linkin yli. WLAN-standardi, jota tukiasema käyttää, on 802.11n. Next-Meshin reititin sisältää VPN-palvelimen, johon saadaan yhteys tukiaseman välityksellä. Testauksessa siis luotiin WLAN-yhteys tukiasemaan, joka puolestaan välitti signaalin langallisen ethernetin yli reitittimelle, josta yhteys jatkui joko suoraan internetiin tai VPN-palvelimen kautta internetiin.

VPN-yhteys muodostettiin asiakasohjelmilla Windowsilla, Linuxilla, Androidilla ja Windows Phonella. Tehtävään soveltuvia asiakasohjelmia on runsaasti, mutta testauksessa pitäydyttiin mahdollisimman yksinkertaisissa ohjelmistoissa, mieluiten OpenVPN-derivaateissa. Windows 7:llä kokeiltiin sekä OpenVPN:n avoimen lähdekoodin asiakasohjelmaa. Asiakasohjelman asetuksiin ei juuri tarvinnut kajota. VPN-asiakasohjelmaan syötettiin VPN-palvelimen IP-osoite, jonka jälkeen yhteys voitiin muodostaa.

Android 4.0:sta lähtien on käyttöjärjestelmään kuulunut VPN-asiakasohjelma. Testattiin tätä hyvin pelkistettyä ohjelmaa yhteyden muodostamiseen onnistuneesti. Lisäksi testasimme OpenVPN:n Linux-versioon perustuvaa ICS-OpenVPN-ohjelmaa, joka tarjosi käyttäjäystävällisemmän käyttöliittymän, johon kuitenkin sisältyi kaikki mahdolliset asetusvaihtoehdot. Androidin mukana tuleva VPN-ohjelman käyttö vaati huomattavasti vähemmän resursseja laitteistolta, mikä voi vaikuttaa positiivisesti asiakaslaitteen akkukestoon. ICS-OpenVPN on kuitenkin erittäin hyvä vaihtoehto, joka tekee VPN-yhteyden muodostamisen asiaan perehtymättömälle käyttäjälle helpommaksi.

Windows Phonelle on vuoden 2014 aikana tulossa käyttöjärjestelmään sisältyvä VPN-asiakasohjelma. Toistaiseksi kolmannen osapuolen tarjoamia VPN-asiakasohjelmia ei ole tarjolla; syynä tähän on käyttöjärjestelmärajoitukset. VPN-yhteyden luominen Windows Phonella vaatii teknisiä erityisjärjestelyjä, jolloin ei pystytä takaamaan yhteensopivuutta yleisimpien VPN-tekniikoiden kanssa.

Linuxin testaus suoritettiin Kali-Linux ohjelmistojakelulla, jolla myös tietoturvahyökkäykset suoritettiin. VPN-yhteysohjelma oli tässäkin tapauksessa OpenVPN:n jäsenten avointa lähdekoodia. Asennus ja asetusten mukauttaminen vaativat hieman enemmän työtä kuin Windowsissa, syynä tähän oli enemmänkin testaajien välttävät Linux-taidot kuin ohjelmiston vaikea käyttö. Tulos oli odotetusti positiivinen ja yhteys saatiin ensimmäisellä yrityksellä toimimaan.

Kali-Linuxin avulla yritettiin myös salakuunnella WLAN-liikennettä, mutta liikenne oli liian vaikea purettavaksi luettavaan muotoon. muotoon. Työkaluja VPN-protokollalla suoritetun

salauksen purkuun ei suoraan ole tarjolla. Eri salausalgoritmeja sen sijaan voidaan purkaa, mutta tämäkään ei ole yksinkertainen tehtävä. Parhaimmaksi todettu tapa murtaa VPN-salaus on käyttää ”man-in-the-middle”-tyyppistä hyökkäystä, jossa kaapataan verkkoliikenne siten, että liikenne kiertää salakuuntelijan laitteiston kautta, jolloin suoritetaan liikenteen salaus ja purku molempiin suuntiin. Tämäkään hyökkäys ei toimi valveutunutta käyttäjää vastaan, mikäli käyttäjä huomaa kahden langattoman verkon päällekkäisyyden tai VPN-palvelimen väärän sijainnin verkkotopologiassa.

Yhteyden toimivuutta kokeiltiin kaikilla testialustoilla selaamalla internetiä, FTP tiedonsiirrolla, sekä telnet-yhteyksillä. Androidilla telnet-yhteyttä ei saatu kulkemaan VPN-tunnelissa, vaan tämä yhteys kulki VPN-yhteyden rinnalla salaamattomana. VPN-tunneloinnin vaikutusta siirtonopeuksiin ei aikarajoitteiden vuoksi testattu. Siirtonopeuksiin vaikuttaa moni asia ja asiaa voi lähestyä usealta kannalta. Tämän opinnäytetyön puitteissa olisi VPN- ja salausprotokollien aiheuttama datamäärän kasvu ollut tärkein tutkimuskohde, mutta tässä on kuitenkin kyse marginaalisista kasvumääristä joiden mittaaminen todennäköisesti vaatisi suurta panostusta.

6 VPN-ohjelmistototeutus

Verkkotekniikoiden rinnalla tutkittiin ohjelmistototeutusta Androidille. Tarkoituksena oli luoda OpenVPN:ään pohjautuvasta ICS-OpenVPN-ohjelmasta asiakasyritys NextMeshille räätälöity VPN-asiakasohjelma. Ohjelmistototeutuksen päämäärä oli tarjota NextMeshin WLAN-verkkoasiakkaille mahdollisimman yksinkertainen yhteysohjelma, joka kytkeytyisi päälle aina laitteen yhdistäessä NextMeshin verkkoon.

VPN-ohjelmistototeutusta ei saatettu loppuun. Käytännössä niin ICS-OpenVPN:n kuin muidenkin OpenVPN avointen lähdekoodien hyväksikäyttö kaatui heikkoon tai olemattomaan dokumentaatioon. Kaikkiaan tutustuttiin neljään eri avointa OpenVPN lähdekoodia käsittelevään lähteeseen. Näistä ei kuitenkaan päästy perille NextMeshin ammattikoodaajienkaan avustuksella. Debugging, eli virheiden korjausvaiheessa dokumentoinnin puutteet vaikeuttivat useiden virheilmoitusten ratkaisua.

ICS-OpenVPN:n käyttöliittymä on toteutettu Java-ohjelmointikielellä ja ohjelman ytimessä toimii OpenVPN:n C-pohjainen miniVPN:ksi ristitty verkkoyhteyksistä vastaava ohjelma. ICS-OpenVPN:n Androidille luoma saksalainen ohjelmoija, Arne Schwabe, on myös osallistunut OpenVPN:n kehitykseen. Schwaben ICS-OpenVPN on haarautunut useammaksi erilliseksi ohjelmaksi, sillä ICS-OpenVPN oli ensimmäinen OpenVPN-yhteysohjelma Androidille.

6.1 VPN-ohjelmistototeutuksen rajaukset

Opinnäytetyön Android-mobiilisovelluksen aihevalinta muodostui asiakkaan tarpeesta kyseiselle sovellukselle. Hankkeen onnistuessa työstä olisi hyötynyt niin asiakas kuin verkkovierailijatkin. Android on asiakkaan hotspot-verkoissa toiseksi käytetyin asiakassovellusalusta. Muut käyttöjärjestelmät rajattiin edeltävästä syystä opinnäytetyön ulkopuolelle. Sovellus on kuitenkin toteutettavissa kaikille käyttöjärjestelmille. Käytännössä Androidin lisäksi muun muassa IOS käyttöjärjestelmälle ja Windows Phonelle sovellus olisi toteutettavissa. Androidia lukuun ottamatta muut käyttöjärjestelmät kuitenkin rajattiin asiakkaan toivomuksesta pois ja keskityttiin Android sovellukseen. PfSense verkonhallintaohjelmiston avulla Android sovellukseen voisi myös liittää automaattisen tunnistuksen käyttäjän käyttöjärjestelmää koskien. Näin VPN-WLAN-tietoturvasovellus käynnistyisi automaattisesti käyttäjän ollessa hotspot-verkon läheisyydessä. (NextMesh International 2013.)

Opinnäytetyön hankkeistetun toteutuksen ongelma on langattoman verkon nykyinen turvattomuus käyttäjille. Tämä asettaa opinnäytetyölle kehykset, joiden puitteissa toimitaan. Ongelmasta saadaan myös aihe uuden kehittämiselle. Avoin lähdekoodi aiheena on ollut ajankohtainen koskien mm. Yhdysvaltojen NSA:n ja Iso-Britannian GCHQ:n tiedustelupalvelua NAC (Network Analysis Centre). (Hyppönen 2013.)

VPN-ohjelmisto on toteutettavissa useille mobiilikäyttöjärjestelmille. Näitä ovat mm. iOS, Windows Phone ja Android. Erittäin yleinen Samsung Android-käyttöjärjestelmänsä kanssa on loogisin valinta toteutukselle, tämä on myös asiakkaan toive. Toteutukseen voisi myös lisätä pfSense tunnistimen, joka NextMesh International WLAN-verkon havaitessaan käynnistäisi VPN-ohjelman automaattisesti.

IPadin iOS käyttöjärjestelmä tukee kolmea erilaista virtuaalista yksityisverkkoa (VPN). Näistä ensimmäinen on OSI–mallin toisella tasolla toimiva tunnelointiprotokolla (L2TP). Toinen on pisteestä pisteeseen tunnelointiprotokolla (PPTP) ja kolmas on Ciscon IPSec (IP Security Architecture), eli turvaprotokolla. Esitellyt virtuaaliverkot toimivat lähes samalla tavalla keskenään. IPadin käyttämä VPN, ja verkkoon asennettu VPN, johon iPad on ottamassa yhteyttä, määrittelevät oikeat asetukset salatulle verkkovierailulle. IPad tukee myös SSL (Secure Sockets Layer) VPN:n tietoverkkokryptausprotokollaa. SSL-protokollaa käytetään myös verkkosivustoilla, kun halutaan salainen yhteys luottamuksellista tiedonsiirtoa varten. SSL-protokollan ollessa käytössä, on verkkoyhteys turvattu pahantahtoisilta urkkijoilta. IPad tukee SSL VPN-yhteyksiä Juniper, Cisco ja F5 yrityksiltä. IPadille voi myös koodata oman SSL-VPN-tuen niin halutessaan. (Welch 2011.)

Windows Phonelle sovellus olisi tehtävissä C#-, C++- tai Visual Basic ohjelmointikielillä WP 8.1 versiosta eteenpäin. Windows Phone Storen ja Windows Phone SDK paketin asentamalla on Windows Phonelle mahdollista työstää kyseinen tietoturvasovelluksen versio. (Microsoft 2013.) Ilmeistä on, että sovellus tullaan teettämään useille eri käyttöalustoille vuosien 2014-2015 aikana NextMesh Internationalin toimesta.

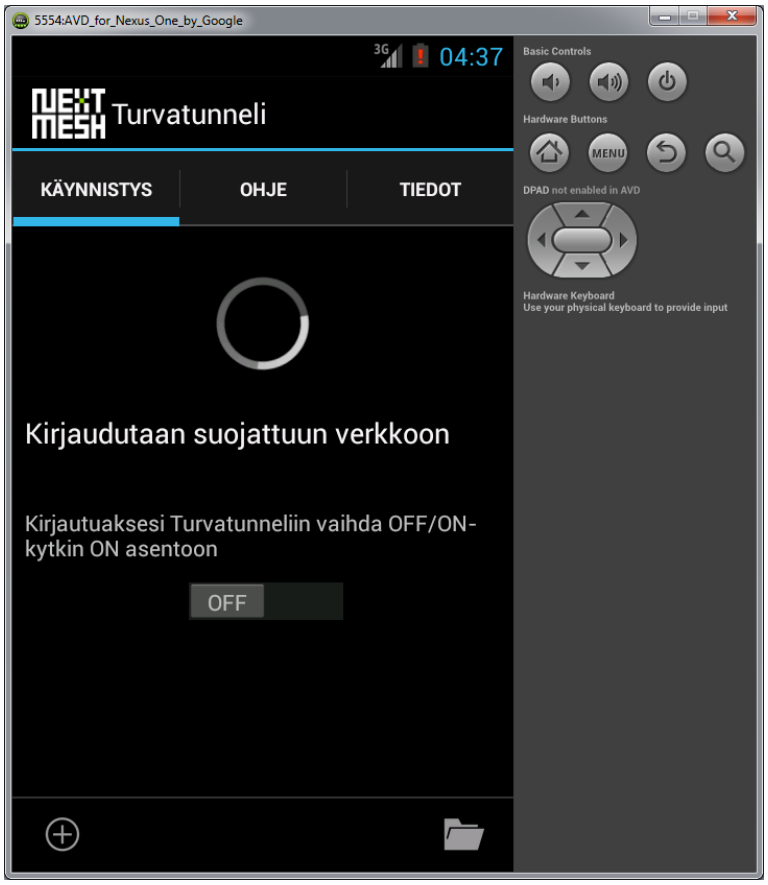
6.2 VPN-käyttöliittymän kehykset

Asiakasyritys tarjosi kehityskohteen VPN-WLAN-tietoturvasovelluksen luomisesta. Kyseisen sovelluksen Androidille oli oltava helppokäyttöinen, sillä käyttäjiä ei sovi kiusata monimutkaisella sovelluksella. Mikäli käyttäjä ei koe sovelluksen käyttöä helpoksi tai asennus on vaivalloinen, voi turvallisuutta parantava sovellus jäädä kömpelyytensä vuoksi kokonaan käynnistämättä. Käyttöliittymän on oltava ilmiselvä heti ensi vilkaisusta lähtien. Yhdenmukaisuus olemassa olevien yksinkertaisten käyttöliittymien kanssa on tärkeätä. (Krug 2006.)

Kuva 13: VPN-yhteysohjelman MS Visiolla tehty rautalankamalli

Microsoftin Visiolla luotiin mahdollisimman yksinkertainen malli, johon VPN-yhteysohjelman käyttöliittymä perustuisi. Taustavärinä musta säästää näytöllä virtaa verrattuna valkoiseen.

Korkea kontrasti yhdessä ilmavaan asetteluun tekee kokonaisuuden hahmottamisesta helpompaa.
Käyttöliittymän helppokäyttöisyys tulisi luoda erittäin selkeällä visuaalisella toteutuksella. Android-sovelluksessa käyttäjä näkee NextMesh Internationalin logot ja VPN OFF/ON (ks. kuva 14) kosketuksella vaihtuvan kytkimen. Välisivuja sovelluksessa on pääsivun lisäksi kaksi: käyttöohjeet ja sovelluksen tiedot. Taustavärinä on musta, joka sopii hyvin Googlen suosittelemaan Holo-ulkonäköön. (Powell 2012.) Visuaalisuus päätettiin yhdessä NextMesh Internationalin kanssa. Lisäksi sovelluksen tulisi optiona näyttää VPN-yhteyden tila.



Kuva 14: Toteutunut käyttöliittymä AVD-virtuaalilaitteessa

Sovellukseen ei tarvitse erikseen kirjautua käyttäjätunnuksella ja salasanalla. Erillisiä käyttäjiä ei yritetäkään tunnistaa. Sovelluksen asetukset ovat esimääritettyinä Android-sovelluspaketissa (APK) conf- tai ovpn-tiedostoina ja uudet tai muuttuneet yhteysasetukset jaetaan käyttäjille ohjelmapäivitysten kautta. (Android Open Source Project 2013.)

6.3 Ohjelmiston rakenne

VPN-tekniikka itsessään on useamman protokollan yhdistelmä. VPN-ohjelmistot hyödyntävätkin usein olemassa olevia valmiita ohjelmisto-osioita toimintaansa täydentämään. VPN-WLAN-

tietoturvasovellus, jota tämän opinnäytetyön aikana työstettiin, perustuu avoimen lähdekoodin VPN-sovellukseen, joka puolestaan perustuu OpenVPN-ohjelmistoon, joka taas puolestaan käyttää useaa muuta ohjelmistoa toimintansa apuna. (OpenVPN 2013.)

Kuva 15: Ohjelmiston rakenne

Kaikki tämän opinnäytetyön aikana itse luotu ja lainattu lähdekoodi on avoimen lähdekoodin lisenssein suojattua. Avointa lähdekoodia hyväksikäyttäen ei kaikkea tarvitse ohjelmoida alusta asti, vaan kokonaisuus voidaan rakentaa ohjelmisto-modulaarisesti.

Android-ohjelman ohjelmointikielenä toimii Java, joka mobiililaitteessa toimii Dalvik-virtuaalikoneessa binäärikäännöksenä (.dex-tiedosto). Kyseessä on sama toimintaperiaate kuin yleensäkin Java-ohjelmistoissa, joissa binäärikäännös toimii alustariippumattomasti Java Runtime Environmentissa (JRE). Android-ohjelman kokonaisuutta ja käyttöliittymää hallitaan XML-tiedostojen kautta. Valmiissa muodossaan Android-ohjelma on yksi zip-pakattu apk-tiedosto, josta löytyy Java-binääritiedostot, XML-tiedostot ja lisäkomponentit kuten kuvakkeet ja tietokantatiedostot. (Android Open Source project 2013.)

6.4 Toteutuksen ohjelmisto

Sovelluksen voi luoda käyttäen pelkkiä skriptejä, jotka hyödyntävät Android-käyttöjärjestelmään sisältyvää VPN-sovellusta. Skriptit ovat komentojonokäskyjä, jotka käyttävät toisien ohjelmien toimintoja hyväkseen. Android-käyttöjärjestelmän komentokehotteen toiminnot (shell) ovat erittäin rajoittuneita. Usein Android-skriptejä varten onkin asennettava erillinen ohjelmistopaketti, joka tarjoaa paremman skriptaustuen. Skriptien toimivuutta eri Android-versioiden välilläkään ei voi taata eivätkä skriptit yleensä toimi Androidissa ilman roottausta. Roottaus tarkoittaa käyttöjärjestelmän muuttamista niin, että ohjelma-asennuksille annetaan oikeudet muuttaa käyttöjärjestelmän tietoja. (Android-scripting 2013.)

ICS-OpenVPN on OpenVPN:ään perustuva Android sovellus. OpenVPN:n runsas lähdekoodi ja sen hyvä ohjeistus tarjoaa hyvän pohjan uuden sovelluksen kehittämiseen. OpenVPN on kuitenkin huomattavasti raskaampi työstää kuin skriptien luonti Androidin omalle VPN-ohjelmalle. Open-VPN:n ja ICS-OpenVPN:n lähdekoodeja hyväksikäyttäen pitäisi tuloksen kuitenkin olla huomattavasti laadukkaampi ja luotettavampi. (Schwabe 2013.)

Muutokset ICS-OpenVPN koodissa kannattaa kohdistaa käyttöliittymään ja uuteen asetusten-hallintaan. Käytännössä tämä tarkoittaa asetusten automaattista hakua konfiguraatiotiedostosta, joka sisällytetään APK-tiedostoon, ja asetusten piilottamiseen käyttäjältä. Edes käyttäjätunnuksella tai salasanalla ei pitäisi häiritä käyttäjää, vaan istunnot todennettaisiin sertifikaatein. Lopputuloksena pitäisi olla käyttöliittymä, joka rajoittuu päälle/pois-nappiin.

Jatkokehitysideoista tärkeimmäksi nousisi automaattinen yhteydenotto NextMesh Internationalin hotspot-verkon kautta VPN-palvelimeen. Tällöin sovellus jäisi taustalle tarkkailemaan langattomia verkkoja. Ohjelman tunnistaessa NextMesh Internationalin verkon, ohjelma avaisi automaattisesti VPN-yhteyden WLAN-verkon yli. Tämän toteutus on Android-kehitysympäristön puitteissa mahdollista. (Android Open Source project 2013.)

6.5 Ohjelmistonkehitysympäristö

Androidilla oli pitkään kehitysalustana ADT (Android Developer Tools), joka on Androidin SDK (Software Development Kit), eli ohjelmistonkehityspaketti. ADT sisältää API-kirjaston (Application Programming Interface), eli ohjelmointi-rajapinnan. Lisäksi pakettiin on sisällytetty monia tarpeellisia työkaluja, joita tarvitaan kehityksen-aikaisessa testauksessa. ADT muuttui joulukuussa 2013 Android Studioksi, joka nykyisin on käytössä.

Kehityspaketin komponentteja hallitaan omalla ohjelmalla. Jokaiselle Android-versiolle on oma rajapintansa joka ladataan hallintaohjelmalla erikseen. Asennettaviin optioihin kuuluu myös Android-lähdekoodi, esimerkkiohjelmat ja avustavat lisädokumentit. (Android Open Source project 2013.)

AVD (Android Virtual Device) on emulaattori, jossa voi ajaa hallintaohjelmistolla ladattuja järjestelmäkuvia (Android system image). Emulaattori esittää aitoa Android-laitetta. AVD:n avulla pystytään testaamaan ohjelmien toimintaa virtuaalisissa laitteissa. Virtuaalilaitteista löytyy esimerkkiasennuksina Google Nexus-puhelimet ja omien laitteiden luominen on tehty erittäin helpoksi. Ikävä kyllä emulaattori on erittäin raskas ajaa jopa modernilla pöytäkoneella. (Android Open Source project 2013.)

6.6 Vaihtoehtoiset toteutukset

Skriptirajapinnan puute Androidissa estää komentojonopohjaisen VPN-yhteystoteutuksen. Tämän tyyppinen ratkaisu olisi kuitenkin tehokas eikä vaatisi paljon laiteresursseja. Jotta Android tukisi skriptejä, on asennettava erillinen ohjelma, joka mahdollistaa Linux-tyyppiset komentojonot. Scripting Layer for Android (SL4A) on asennettavissa vain, mikäli Android-

käyttöjärjestelmä on niin sanotusti rootattu. Tämä itsessään on tietoturvariski, eikä missään nimessä tavallisen käyttäjän kykyjen ulottuvilla.

Teoreettisesti olisi kuitenkin mahdollista luoda skripti, joka käynnistäisi VPN-ohjelman ja ottaisi suoraan yhteyden skriptin määrittämään VPN-palvelimeen. Tämä ei vaatisi kovinkaan kummoisia ohjelmointitaitoja. Esimerkiksi ICS-OpenVPN saataisiin yhdistettyä VPN-palvelimeen seuraavanlaisella komennolla: *am start -a android.intent.action.MAIN -n de.blinkt.openvpn/.LaunchVPN -e de.blinkt.openvpn.shortcutProfileName Home*.

Vuoden 2013 lopussa ICS OpenVPN sai päivitysten myötä AIDL-toiminnon. AIDL, eli Android Interface Definition Language, on ohjelmistojen väliseen kommunikointiin tähtäävä rajapinta. Androidin ohjelmat ovat normaalisti täysin eristyksissä toisistaan ja ohjelmien välinen kommunikointi on mahdollista vain monimutkaisten välikäsien kautta. (AOSP 2013.)

AIDL yhdessä ICS OpenVPN:n kanssa mahdollistaisi yksinkertaisen Android-ohjelman luomisen, jonka ainoa toiminto olisi käskyjen välittäminen ICS OpenVPN:lle. Käskyt suoritettaisiin yhden tälle tarkoitetun luokan kautta. ICS OpenVPN:n vastaanottaisi käskyt AIDL-rajapinnan kautta.

```
public class StartOpenVPNActivity extends Activity {
@Override
  public void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.main);
    final String EXTRA_NAME = "de.blinkt.openvpn.shortcutProfileName";
    Intent shortcutIntent = new Intent(Intent.ACTION_MAIN);
    shortcutIntent.setClassName("de.blinkt.openvpn", "de.blinkt.openvpn.LaunchVPN");
    shortcutIntent.putExtra(EXTRA_NAME,"upb ssl");
    startActivity(shortcutIntent);
  }
}
```

Taulukko 2: AIDL-esimerkki ICS-OpenVPN (Arne Schwabe 2013.)

7 Yhteenveto

Opinnäytetyössä keskityttiin käyttäjää lähinnä olevan fyysisen verkkotietoturvan, eli langattoman lähiverkon, suojaamiseen. Osaksi tutkittiin käytettyjä tekniikoita ja tehtiin käytännön kokeita, jotka vahvistivat tutkimuksen aikana syntyneitä epäilyjä. Eli yleiset suojaustekniikat murtuvat hyvinkin helposti. Osatavoitteena oli luoda yleishyödyllinen mobiilitietoturvaohjelma. Yleiskäyttöön valmista tuotetta ei tästä syntynyt.

Käyttäjän yksityisyys langattomissa lähiverkoissa on haavoittuvaista. Datan salakuuntelulta julkisissa WLAN-verkoissa ei itsestään suojaa mikään. Julkiset WLAN-verkot ja niissä siirretty informaatio, kuten yksityiset sähköpostit tai sosiaalisen median viestit, eivät ole suoraan turvassa salakuuntelulta.

WLAN-hotspotteja, eli avoimia langattomia verkkoja maailmalla on useita. Harvemmin on kuitenkaan muistettu ottaa huomioon tietoturva. Ratkaisua, jota tämän työn aikana etsittiin, voidaan toivottavasti käyttää laajemminkin langattomien verkkojen asiakkaiden turvaksi. WLAN-hotspotteja palveluna tarjoava asiakasyritys oli jo ennen tätä toimeksiantoa suunnitellut mahdollisia toteutustapoja. VPN:n käyttäminen avoimissa langattomissa verkoissa paremman tietosuojan tarjoamiseksi ei sellaisenaan kuitenkaan riitä, vaan sen on myös oltava helppoa. Tähän tarpeeseen sovitimme opinnäytetyönä toteutettavaksi selvityksen teoriasta ja ohjelmistoista sekä käytännön testauksesta.

VPN-yhteyksien toivoisikin siirtyvän yritysverkoista laajemmin yksityishenkilöiden käyttöön. Lähitulevaisuudessa verkko-operaattorit saattavat tarjota yksityishenkilöille VPN-palveluja, jotka parantavat tietoturvaa ja mahdollistavat turvallisen yhteyden mobiililaitteen ja kodin välille. Näitä yhteyksiä tarjoavat tällä hetkellä monet ulkomaiset toimijat, mutta Suomen osalta tarjontaa ei vielä paljoa löydy.

Tutkittaessa verkkoprotokollia ja suojaustekniikoita kävi ilmi, että moni jokapäiväiseen tietoliikenneyhteyksiin käytettävä standardi on jo kymmenen vuoden ikäinen. Jopa WLAN-verkkojen tuorein suojausprotokolla, WPA2, on aikansa elänyt. Yhdistelemällä näitä ikääntyviä tekniikoita voidaan lisätä turvallisuutta, mutta yksinkertaistamalla voidaan päästä parempaan tulokseen. VPN-suojaustekniikkaa käyttämällä yhdistäen vahvoja salausalgoritmejä ja sertifikaatteja voidaan luoda yksityiskäyttäjälle erittäin turvallinen verkkoyhteys. Tämä yhteys voidaan luoda jopa niin, että VPN-tunneli on käytössä mobiililaitteella riippumatta siitä, käytetäänkö internetliittymänä mobiililaajakaistaa tai kauppakeskuksen tarjoamaa WLAN-yhteyttä.

Parhaimmillaan VPN-yhteys ei hidasta verkkokäyttöä, mutta mikäli VPN-palvelin sijaitsee pitkän yhteyden takana, esimerkiksi toisessa maanosassa, ovat huomattavat viiveet yhteydessä odotettavia. Varsinkin VPN-ilmaispalvelimet kärsivät hitaudesta, mutta kaupallinen palvelu ei tietenkään takaa nopeaa yhteyttä. Kotireitittimellä luotu VPN-yhteys on teknisen taitajan ratkaisu, joka nykylaitteilla onnistuu nopeasti. Monet modeemi-reitittin yhdyslaitteet suurimmilta valmistajilta tarjoavat VPN-palvelimen laitteen ohjelmistossa. Tämän tyyppinen omatoiminen ratkaisu tarjoaa monia hyviä puolia yhteysnopeudesta aina tiedostopalvelimen saatavuuteen asti.

Useampaa laitealustaa kokeilemalla voitiin todeta, että VPN-yhteys todellakin tarjoaa lisäturvaa. Salakuuntelua NextMeshin testilaitteistolla suorittaessa huomattiin selkeä ero eri salaustekniikoissa. Parhaaksi todettiin VPN-yhteys. HTTPS-protokollan käyttämä SSL/TSL-salaus, jota käytetään verkkosivuille kulkevan liikenteen suojaamiseksi, tarjoaa myös hyvän suojan. HTTPS-yhteys voidaan kuitenkin teoriassa kaapata ohjaamalla asiakas kloonisivulle, joka toimii oikean sivuston ja asiakkaan välillä.

WLAN-verkkojen suojaukseen käytettävä WPA2 on suojaustasoltaan huolestuttavan helposti murrettavissa. Missään nimessä tätä suojausta ei kuitenkaan pidä olla käyttämättä. WPA2 luo kuitenkin suojauksen, joka estää vahingossa tapahtuvan tietovuodon.

Asiakasyritykselle tarjouduttiin luomaan sovellus, joka toimisi Android-laitteissa ja tarjoaisi yhdellä napinpainalluksella VPN-yhteyden, kun laite olisi NextMeshin tarjoaman WLAN-verkon alueella. Android-tietoturvasovelluksen ohjelmointi esiintyi ajoittain haasteellisena. Ratkaisuihin saatiin tukea keskustelufoorumeista ja asiakkaan toimesta. Myös pitkä toteutusaika pakotti päivittämään Android-kehitysalustan Eclipse-alustasta Android Studioon. Tämän vuoksi ADT:lla työstetty GUI (Graphical User Interface) ei yhteensopivuussyistä toiminut Android Studion kanssa.

ICS OpenVPN:n lähdekoodin olematon dokumentaatio ja harvat kommentit olivat yksi suurimmista haasteista. Koodia seuraamalla pystyttiin ymmärtämään useimmat ohjelman funktiot, mutta kokonaisuuden hahmottaminen oli mahdotonta. Yksittäisten funktioiden etsiminen oli työlästä, eikä aina onnistunut. Lopulta otettiin yhteys ICS OpenVPN:n luojaan, jotta olisi saatu selvyyttä toimintoihin ja apua ohjelman editoimiseen. Ymmärrys ei kasvanut niukkojen vastausten perusteella, joten avuksi otettiin NextMesh. Tietämys ei ICS-OpenVPN:n dokumentoinnin puutteiden vuoksi kasvanut heilläkään koodista. Funktiot löytyivät osittain, mutta kokonaisuuden hallinnan ymmärtämiseksi osoittautui kannattamattoman suureksi henkilötyöpäivienkin osalta. Tämän vuoksi päädyttiin valmiiden OpenVPN-sovellusten testaukseen.

NextMeshille tarkoitettua ohjelmistoa ei saatu päätökseen. Ohjelmistonkehityksestä tuli kuitenkin opittua paljon. Kehitysympäristöt, versionhallinta ja lähdekoodin jakaminen verkkopalveluiden kautta olivat asioita, jotka oli opeteltava mittavan ohjelmointiprojektin hallitsemiseksi. Ohjelmankehityksen päättäminen ennen valmistumista oli raskas päätös, mutta tässä tapauksessa oikea. Aikaa olisi vielä kulunut paljon ennen toimivan ohjelman valmistumista eikä lopputulos olisi tarjonnut lisäarvoa suhteessa tarvittaviin resursseihin.

Tulevat käyttöjärjestelmäpäivitykset mobiilipuolella lupaavat tuoda natiivin VPN-tuen kaikille käyttäjille (Anandtech 2014). Käyttöliittymä ja hallinta ovat kuitenkin vielä toissijaisia, joten peruskäyttäjille ei tästä vielä ole tietoturvaratkaisuksi (Android Developers 2014). Päivitykset

tarjoavat kuitenkin pohjan, jolle kolmannen osapuolen ohjelmistovalmistajat voivat rakentaa helppokäyttöisempiä palveluja.

Jatkotutkimuksia salausprotokollien ja VPN-yhteysprotokollien aiheuttamasta lisäkuormasta olisi mielenkiintoista nähdä. Tulevaisuudessa voidaan olettaa tarvittavan vahvempia salausalgoritmejä, jolloin sisällön suhteellinen osuus pienenee ja siirrettävä datamäärä kasvaa. Vaikka kyse on hyvin pienestä kasvusta, tulisi tämä ottaa huomioon tulevia tiedonsiirtoprotokollia suunniteltaessa. Kaiken kaikkiaan tulisi verkkoprotokollien tulevaisuudessa pystyä tarjoamaan vaihtelevalla salausvahvuudella suojattu tiedonsiirto, jotta verkkoliikenteen paketointia saadaan yksinkertaistettua.

Odotetusti 802.11-standardien tarjoama turva voitiin todeta riittämättömäksi. WLAN-verkkojen käyttäjät ovat aina vaarassa, mikäli ainoana turvana on WPA tai WPA2. IEEE:n standardien kehitys on tietoturvallisuuden osalta saanut liian vähän huomiota. Olisikin tärkeää, että tulevaisuudessa kaikille verkkokäyttäjille olisi tarjolla yhtenäinen salaustekniikka, joka toimisi kaikissa verkoissa. Toistaiseksi voi vain suositella VPN-yhteyksien käyttämistä.

Verkkokäyttäjien huoleton suhtautuminen tietoturvaan on edelleen suuri ongelma, johon ei ratkaisua ole nähtävissä, ennen kuin laite- ja ohjelmistovalmistajat kykenevät tarjoamaan automaattisen, käyttäjälle näkymättömän salauksen. Harva verkkokäyttäjä ymmärtää tietojensa arvoa ennen kuin näitä tietoja käytetään väärin rikollisen toimesta. Tietoturvallisuuden tiedostaminen ja verkkokäyttäytyminen ovat jo nyt tärkeitä kansalaistaitoja, joita ei vielä peruskouluissa opeteta.

Lähteet

Kirjalliset lähteet:

Allen, J.H. 2002. *Verkkotietoturvan hallinta - CERT.* Helsinki: Edita Prima. Sivut 401, 407.
Bartz, R. 2012. *CWTS: Certified Wireless Technology Specialist Official Study Guide: (PW0-071) (2nd Edition).* Somerset NJ, USA: Wiley. Sivut 303, 317 – 320.
Held, G. 2004. *Virtual Private Networking.* West Sussex, England: John Wiley & Sons LTD. Sivut 1 - 18, 79 - 189.
Järvinen, M. 2013. Kick-off palaveri. Haastattelu 31.5.2013.
Järvinen, P. 2003. *Salausmenetelmät*. Jyväskylä: Docendo. Sivut 159 - 162, 255 - 256.
Krug, S. 2006. *Don't Make Me Think - A Common Sense Approach to Web Usability.* 2nd edition. Berkeley, California: New Riders Publishing. Sivut 20 - 52.
Perlmutter, B. & Zarkower, J. 2001. *Virtuaaliset yksityisverkot.* Helsinki: Edita. Sivut 48, 141 – 147, 158, 155.
Salmenkylä, R. 2012. Tietoverkkoarkkitehtuuri. Laurea Leppävaara, Espoo.
Strebe, M. 2004. *Network Security Foundations*. CA, USA: Sybex. Sivut 48 – 50.
Welch, J. 2011. VPNs AND THE iPAD. *Macworld.* Vol. 28 Issue 7. Sivut 38 – 39.

Sähköiset lähteet:

Al Shourbaji, I. 2013. An Overview of Wireless Local Area Networks. Viitattu 23.8.2013.
http://arxiv.org/ftp/arxiv/papers/1303/1303.1882.pdf
Ala-Mutka, K., Palviainen, J., Rintala, M. & Savikko, V 2002. 19.2 OSI-malli. Viitattu 24.6.2013.
http://www.cs.tut.fi/etaopetus/titepk/luku19/OSI.html#fyysinen
Anchorfree. 2013. Benefits of VPN. Viitattu 26.6.2013.
http://www.hotspotshield.com/benefits-of-vpn
Android Developers. 2014. VpnService. Viitattu 8.4.2014.
http://developer.android.com/reference/android/net/VpnService.html
Android Open Source project. 2013. A Detailed Look at the Build Process. Viitattu 26.8.2013.
http://developer.android.com/tools/building/index.html
Android Open Source project. 2013. Application Fundamentals. Viitattu 27.8.2013.
http://developer.android.com/guide/components/fundamentals.html
Android Open Source Project (AOSP). 2013. Android Interface Definition Language (AIDL). Viitattu 20.1.2014.
http://developer.android.com/guide/components/aidl.html
Android Open Source project. 2013. Android.net.wifi. Viitattu 27.8.2013.
http://developer.android.com/reference/android/net/wifi/package-summary.html
Android Open Source project. 2013. Get the Android SDK. Viitattu 27.8.2013.
http://developer.android.com/sdk/index.html
Android Open Source project. 2013. Getting Started with Android Studio. Viitattu 27.8.2013.
http://developer.android.com/sdk/installing/studio.html
Android Open Source project. 2013. Using the Emulator. Viitattu 27.8.2013.
http://developer.android.com/tools/devices/emulator.html
Android-scripting. 2013. Scripting Layer for Android brings scripting languages to Android. Viitattu 27.8.2013.
https://code.google.com/p/android-scripting/
Cisco. 2012. The Future of Hotspots: Making Wi-Fi as Secure and Easy to Use as Cellular. Viitattu 9.1.2014.
http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns673/white_paper_c11-649337.pdf
DD-WRT. 2014. About DD-WRT. Viitattu 7.4.2014.
http://www.dd-wrt.com/site/content/about
Eli the Computer Guy. 2013. Personal VPN Services for Security Overview. Viitattu 14.8.2013.
http://youtu.be/5e_gsGoNOf4
Goodin, D. 2013. Stop using NSA-influenced code in our products, RSA tells customers. Viitattu 10.1.2014.

http://arstechnica.com/security/2013/09/stop-using-nsa-influence-code-in-our-product-rsa-tells-customers/
Howse, B. 2014. Microsoft Announces Windows Phone 8.1.Viitattu 8.4.2014.
http://www.anandtech.com/show/7920/microsoft-announces-windows-phone-81
Hyppönen, M. 2013. Kuinka NSA petti maailman luottamuksen – aika toimia. Viitattu 9.1.2014.
http://www.ted.com/talks/lang/fi/mikko_hypponen_how_the_nsa_betrayed_the_world_s_trust_time_to_act.html
Hänninen, K. 2008. tikolyhennetty_ontohje.doc. Viitattu 25.6.2013.
https://optima.discendum.com/learning/id74/bin/doc_show?id=1174283&ws=1152869&noedit=1&name=/tikolyhennetty_ontohje.doc
IEEE. 2007. IEEE Std 802.11™-2007 (Revision of IEEE Std 802.11-1999). Viitattu 16.7.2013.
http://standards.ieee.org/getieee802/download/802.11-2007.pdf
Koivunen, E. 2010. Langattomat lähiverkot. Viitattu 20.6.2013.
https://www.vahtiohje.fi/web/guest/langattomat-lahiverkot
Lanning, K. 2007. WI-FI GUEST ACCESS: A STRUGGLE FOR SECURE FUNCTIONALITY IN ACADEMIC ENVIRONMENTS. Chapel Hill NC, USA. Viitattu 25.6.2013.
https://cdr.lib.unc.edu/indexablecontent?id=uuid:8c43786b-977a-4f54-8d4c-5b1a701ce510&ds=DATA_FILE
Mackall, M. Mercurial SCM. Viitattu 9.7.2013.
http://mercurial.selenic.com/about/
McCann, S.&, Ashley, A. 2013. OFFICIAL IEEE 802.11 WORKING GROUP PROJECT TIMELINES - 2013-11-15. Viitattu 9.1.2014.
http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm
Mercurial community. 2013. Mercurial source control management. Viitattu 26.8.2013
http://mercurial.selenic.com/about/
Meru Networks. 2012. Viitattu 29.8.2013.
http://www.merunetworks.com/products/technology/80211ac/index.html
Microsoft. 2013. Viitattu 12.8.2013.
http://phone.windowsstore.com/developers/ios
Microsoft. 2013. Mitä eroa on keskittimellä, kytkimellä, reitittimellä ja tukiasemalla? Viitattu 13.8.2013.
http://windows.microsoft.com/fi-fi/windows-vista/how-do-hubs-switches-routers-and-access-points-differ
Mitchell, B. How Fast Is 802.11g Wi-Fi Networking?
http://compnetworking.about.com/od/wirelessfaqs/f/howfastis80211g.htm
Mitchell, B. What Is a VPN? Viitattu 20.6.2013.
http://compnetworking.about.com/od/vpn/a/what_is_a_vpn.htm
Mitchell, B. WPA – Wi-Fi Protected Access. Viitattu 27.8.2013.
http://compnetworking.about.com/cs/wirelesssecurity/g/bldef_wpa.htm
NextMesh International Oy. 2013. Viitattu 10.1.2014.
http://nextmesh.fi/
OpenVPN Technologies, Inc. 2013. HOWTO. Viitattu 27.8.2013.
http://openvpn.net/index.php/open-source/documentation/howto.html
OpenVPN Technologies. 2013. Getting Started with Private Tunnel. Viitattu 26.6.2013.
https://www.privatetunnel.com/index.php/kb-installinguninstalling/195-kb-getting-started.html
OpenVPN Technologies. 2013. HOWTO. Viitattu 15.8.2013.
https://openvpn.net/index.php/open-source/documentation/howto.html
Powell, A. 2012. Holo Everywhere. Viitattu 26.8.2013.
http://android-developers.blogspot.fi/2012/01/holo-everywhere.html
Ratol 2002. OSI-malli. Viitattu 13.8.2013.
http://www.ratol.fi/opensource/lahiverkot/fin/yleista/osi_malli.htm
Schwabe, A. 2013. ICS-OpenVPN – OpenVPN for Android 4.0+. Viitattu 27.8.2013.
https://code.google.com/p/ics-openvpn/
Shirer, M. 2013. Worldwide WLAN Market Continues Robust Growth in Second Quarter of 2013, According to IDC. Viitattu 2.9.2013.
http://www.idc.com/getdoc.jsp?containerId=prUS24278113
Spamlaws. 2013. Hacking Into VPN Connections. Viitattu 15.7.2013.
http://www.spamlaws.com/vpn-hack-connection.html

Spamlaws.2013. OSI Models and How They Work. Viitattu 12.8.2013.
http://www.spamlaws.com/how-osi-models-work.html
Spector, L. How Safe is WPA2-Secured WiFi? Viitattu 21.8.2013.
http://www.pcworld.com/article/243713/how_safe_is_wpa2_secured_wifi_.html
The Eclipse Foundation. 2013. Viitattu 9.7.2013.
http://www.eclipse.org/org/
University of Hawaii. 2013. Norman Abramson. Viitattu 15.8.2013.
http://www.ee.hawaii.edu/faculty/detail.php?usr=34
Verkkokauppa.com. 2013. Tukiasemat 300Mbps. Viitattu 27.8.2013.
http://www.verkkokauppa.com/fi/catalog/1727c/Langattomat-Tukiasemat-300Mbps?s=price&o=D

Kuvaluettelo

Kuva 1: OpenVPN Client 16
Kuva 2: WLAN-verkkotopologia 20
Kuva 3: Salaamattoman liikenteen kuuntelu 21
Kuva 4: Tukiasemahuijaus 22
Kuva 5: NextMesh International Oy:n käyttämä Ubiquitin tukiasema 24
Kuva 6: Reititin NextMesh International Oy 25
Kuva 7: Salasanan pituuden vaikutus murtoaikaan 27
Kuva 8: Airmon-ng salakuunteluohjelma 28
Kuva 9: Langattomia verkkoja jotka Airmon-ng löysi testialueelta 28
Kuva 10: Aircrack-ng on löytänyt verkon salasanan. 29
Kuva 11: Fiddler esittää HTTP-liikenteen tiedot helposti luettavassa muodossa 30
Kuva 12: HTTPS-yhteyden tiedot Facebookia käytettäessä 31
Kuva 13: VPN-yhteysohjelman MS Visiolla tehty rautalankamalli 35
Kuva 14: Toteutunut käyttöliittymä AVD-virtuaalilaitteessa 36
Kuva 15: Ohjelmiston rakenne 37
Kuva 16: Ositus ja toteutusvaiheet 49
Kuva 17: Tehtäväluettelo 50
Kuva 18: Aikataulu 50

Taulukot

Taulukko 1: WPA/WPA2-turvatekniikat (Bartz 2012.) 13
Taulukko 2: AIDL-esimerkki ICS OpenVPN:n tekijä Arne Schwabelta 39

Liitteet

Liite 1. Käytetyt lyhenteet 47
Liite 2. Testaussuunnitelma 49

Liite 1. Opinnäytetyössä käytetyt lyhenteet

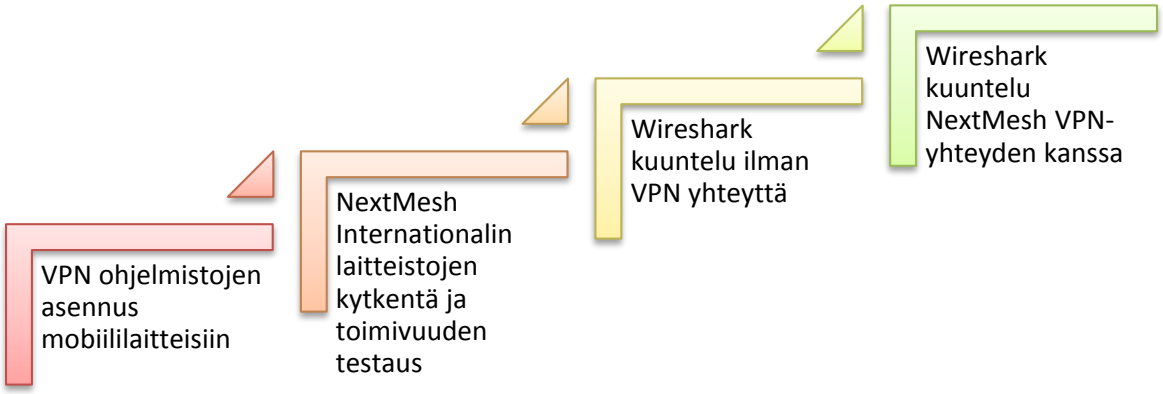
AES	(Advanced Encryption Standard) Rijndael salausalgoritmi
Android	Linux käyttöjärjestelmäydintä käyttävä mobiilikäyttöjärjestelmä
APK	(Application package) Android-ohjelmien tiedostotyyppi
C	Ohjelmointikieli
C#	Microsoftin C:stä jatkokehittämä ohjelmointikieli
C++	C:hen perustuva olio-ohjelmointikieli
CCMP	Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol
DD-WRT	Reitittimen alkuperäisen laiteohjelmiston korvaava Linux-pohjainen ohjelmisto
DEX	(Dalvik Executable) Java-lähdekoodin binäärikäännös Dalvik-virtuaalikoneelle
DHCP	(Dynamic Host Configuration Protocol) IP-osoitteiden hallinnointiprotokolla
Eclipse	Eclipsellä hallitaan avointa lähdekoodia
GRE	(Generic Routing Encapsulation) Ciscon kehittämä IP-tunnelointiprotokolla
HTTP	(Hypertext Transfer Protocol) Applikaatioprotokolla pohja World Wide Web:lle
HTTPS	(Hypertext Transfer Protocol Secure) SSL-salattu HTTP-yhteys
IEEE	(Institution of Electrical and Electronics Engineers) Standardointi organisaatio
iOS	(iPhone OS) Applen kehittämä mobiilikäyttöjärjestelmä
IP	(Internet Protocol) Tiedonsiirtoprotokolla
iPad	Applen mobiililaite
IPSec	(Internet Protocol Security) IP-pakettien turvaprotokolla
ISO	(International Organization for Standardization) Kansainvälinen standardoinnin organisaatioyksikkö
Kernel	Käyttöjärjestelmäydin
LAN	(Local Area Network) Lähiverkko
L2F	(Layer 2 Forwarding Protocol) Cisco Systemsin kehittämä toisen tason tunnelointi protokolla
L2TP	(Layer 2 Tunneling Protocol) VPN:ää tukeva tunnelointiprotokolla
Linux	Monen Unixin kaltaisen käyttöjärjestelmän ydin
Mercurial	Mercurial on avoimen lähdekoodin hallintatyökalu
NAC	(Network Analysis Centre) Britannian tiedustelupalvelu
NAT	(Network address translation) Osoitteenmuunnostekniikka lähiverkon ulkoreunan reittimille
NSA	(National Security Agency) Yhdysvaltain tiedustelupalvelu
OFDM	(Orthogonal frequency-division multiplexing) Modulointitekniikka, jolla dataa siirretään useaa rinnakkaista kantotaajuutta hyväksikäyttäen.
OSI-malli	(Open Systems Interconnection) Seitsemänkerroksinen tietoverkkomalli

pfSense	(Open Source Firewall Distribution) Avoimen lähdekoodin monikäyttöinen verkonhallintaohjelmisto
PoE	(Power over Ethernet) Virta tiettyyn laitteeseen ethernetkaapelia pitkin
PPTP	(Point-to-Point Tunneling Protocol) Pisteestä pisteeseen tunnelointiprotokolla
RC4	Rivest Cipher 4, joka on nimetty RSA Security Ron Rivestin mukaan
Rooting	Android käyttöjärjestelmässä ohjelmien ajamisen mahdollistaminen pääkäyttäjänä. Tämä toiminto voi johtaa takuun umpeutumiseen
RSA	Salausalgoritmi julkisen avaimen salaukseen
SSL	(Secure Sockets Layer) OSI-mallin applikaatiotasolla toimiva kryptausprotokolla
TKIP	(Temporal Key Integrity Protocol) WEP:stä päivitetty WLAN tietoturvaprotokolla
UDP	(User Datagram Protocol) Yhteydetön tiedonsiirtoprotokolla
UTM	(Unified Threat Management) Keskitetty yritysverkon turvaratkaisu
WEP	(Wired Equivalent Privacy) IEEE standardin mukainen turvallisuusalgoritmi
WiFi	(Wireless Fidelity) Langattoman lähiverkkotekniikan kaupallinen brändinimi
WLAN	(Wireless Local Area Network) Langaton lähiverkkotekniikka
WPA	(Wi-Fi Protected Access) WEP:stä päivitetty turvallisuusalgoritmi versio
WPA2	(Wi-Fi Protected Access II) WPA:sta päivitetty turvallisuusalgoritmi versio
VPN	(Virtual Private Network) Virtuaalinen yksityisverkko
ZIP	Häviötön tiedostonpakkausformaatti

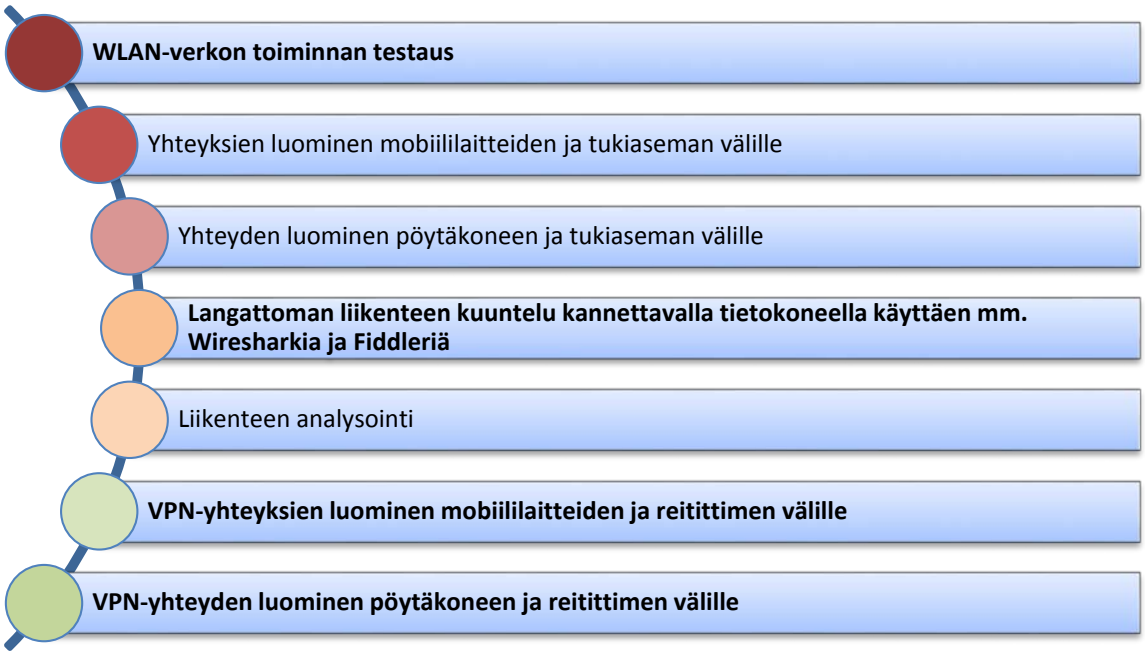
Liite 2. Testaussuunnitelma

VPN WLAN testaussuunnitelma

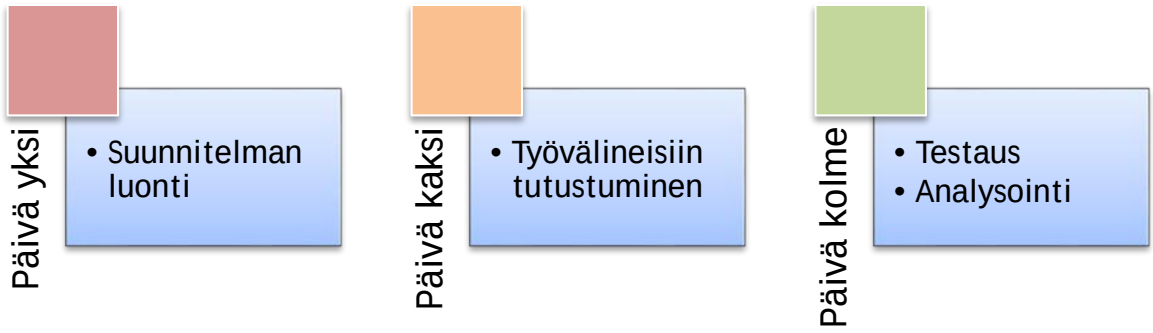
Opinnäytetyötä koskeva toteutuksellinen osuus muutettiin valmiiden ohjelmien testaukseen. Testaukset tehdään NextMesh Internationalin laitteistoilla yksityisessä testausympäristössä. Laitteisto koostuu reitittimestä, jossa on sisäänrakennettu VPN-palvelin. Käytössä on myös WLAN tukiasema. Kyseisten laitteiden avulla testaus saadaan suoritettua ympäristössä, joka vastaa esimerkiksi kauppakeskuksissa olevia verkkoja. Mobiililaitteet ovat Android 4.4 käyttöjärjestelmällä toimiva LG Nexus 5 ja Windows phone 8 käyttöjärjestelmää käyttävä Nokia Lumia 920.



Kuva 16: Ositus ja toteutusvaiheet



Kuva 17: Tehtäväluettelo



Kuva 18: Aikataulu

Riskit

Testausta ei pystytä suorittamaan radioaalloilta täysin suojatussa tilassa. Häiriöitä aiheuttavia langattomia verkkoja on testialueella useita. Tämä saattaa vaikuttaa mm. haluttujen WLAN verkkojen suodatuksen vaikeuteen. Verkkoliikenteen ollessa suojaamattomassa tilassa altistetaan testilaitteisto mahdolliselle salakuuntelulle. Ohjelmistojen toimivuus ja asetusten säätö voi epäonnistua. Haasteena ovat myös langattoman liikenteen kuuntelua varten valitut ohjelmat, jotka ovat testaajille ennestään tuntemattomia. Liikenteen sisällön analysointi voi mm. epäonnistua osittain tai kokonaan. Liikenteestä ei välttämättä saada verkkopakettien tulkinnan avulla tietoturvallisuuden kannalta kriittisiä tietoja selville.

Tavoite

Toteutuksen tavoitteena on testata Android käyttöjärjestelmän VPN-sovellus. Microsoft ei ole toistaiseksi saanut aikaiseksi VPN-asiakasyhteysohjelmaa. Tästä syystä Windows Phone testausta ei tehdä. Testauksen yhteydessä testilaitteeseen asennetaan VPN-asiakasohjelmisto. VPN-yhteyden suojaamaa laitetta kuunnellaan mm. Wireshark verkkoliikenteenkuunteluohjelmalla. Testauksessa VPN-sovelluksen ollessa päällä ja yhteydessä NextMeshin reitittimeen, odotuksena on, ettei langatonta liikennettä pystytä salakuuntelemaan.